2.3. Проблемы идентификации исполнителей и заказчиков кибератак

2.3.1. Введение в проблему

В книге А.И. Белоуса и В.А. Солодухи «Кибероружие и кибербезопасность. О сложных вещах простыми словами», Инфра-Инженерия, 2020, более детально, на конкретных примерах рассмотрены различные концепции, методы, средства организации различных кибератак и разнообразные методы, средства и способы защиты от них. Одним из ключевых моментов для специалистов служб кибербезопасности любой компании является поиск ответа на вопрос – ***а кто и зачем это сделал?***, причем желательно не только *определить* «нападающего», но и *понять* его истинные мотивы, а еще лучше – узнать модератора (заказчика атаки). Как мы покажем ниже, фактически сам процесс решения комплекса подобных задач сегодня больше похож на искусство, чем на науку, хотя в ходе него используются самые современные технические и программные средства и последние достижения науки.

Кажется абсолютно логичным, что прежде чем принимать «ответные меры» по результатам совершенной кибератаки (в последеней редакции национальной стратегии обеспечения кибербезопасности США это называется ***punish*** – наказание, принуждение), надо узнать, а кто это сделал? Но здесь и начинается целый «клубок» проблем. Начнем с того, что «сдерживание» атакующей стороны согласно вышеупомянутой стратегии обеспечения кибербезопасности США должно «сработать» еще до нанесения первого «удара возмездие».

Другие «потенциальные агрессоры» – ***adversaries*** (государства) – должны быть уверены, что «сдерживающее» (наказывающее) государство *точно знает*, кто напал на него. Удар «не того» объекта (человека, организации) не только разрушает логику «принципа сдерживания» (если «невинность» не имеет значения – зачем быть «невинным»?), но и создает нового врага.

Вместо того чтобы ввязаться в одну кибервойну (против «первоначального» нападающего), теперь «наказывающий» (принуждающий) может столкнуться уже с двумя «кибервойнами». Второй «враг» – это та сторона (государство), которая атакующим ошибочно была определена, как «первоначальный атакующий». «Защитник» должен не только убедить себя, но и убедить «третьи лица», что расследование по определению «агрессора» (атакующего) было проведено «правильно» и привести соответствующие аргументы, которые могут рассматривать независимые эксперты (третейский суд).

Но самое главное в этом вопросе – сам «злоумышленник» должен понимать, что процедура выявления его, как «агрессора», действительно выполнена безукоризненно. Ведь если он будет считать, что реально атакованный им объект наносит ответный удар просто «по догадке», или что у него были свои «скрытые мотивы» для «кибердара», очевидно, что он и дальше будет проводить аналогичные атаки независимо от того, будет ли он и дальше подвергаться подобному «наказанию». Необходимость ***«убеждать третьи стороны»*** в правильности определения «агрессора» зависит, можно так выразиться, «от важности» этих «третьих лиц».

Поясним – в отличие от так или иначе установившихся отношений между членами немногочисленного «ядерного клуба», которые даже в периоды «ядерного противостояния холодной войны» *имели специальные средства и неосвещаемые в СМИ специальные каналы взаимодействия и взаимоконтроля*, сегодня в киберпространстве присутствует более ста стран (из более чем 250 подключенных к Интернету), представители которых *предположительно* развивают то, что сегодня мы называем кибероружием, но здесь аналогичные средства и коммуникации напрочь отсутствуют. Злоумышленник должен убедиться, что его «цель» действительно его «вычислила» и именно поэтому нанесла ответный удар – именно потому, что на нее напали.

Здесь следует понимать, что *до сих пор однозначно (убедительно) не установлено*, *кто стрелял в президента Кеннеди*, непонятно даже, был ли это один человек или было несколько выстрелов с разных позиций. Документально не подтверждено утверждение администрации США, что за известной *«атакой 11 сентября»* стоял Бен Ладен. Более того, что касается последнего события, на 750 страницах документального расследования «Аноним. Немысленное. Системный анализ событий 11 сентября 2001 года и того, что им предшествовало», М.: Товарищество научных изданий КМК, 2019 (https://www.bookvoed.ru/book?id=9634306) изложены результаты обширного исследования генезиса американского политико-силового истеблишмента, превратившегося в «корпоратократию нового типа» – реально действующую скрытую политическую власть с далеко идущими глобальными целями, важнейшей отправной точкой которых и стали сгенерированные ими же «события 11 сентября».

Авторы этого фундаментального исследования не только предоставляют детальную картину этого грандиозного преступления начала XXI века, разбирая все его механизмы и артефакты с опорой на официальные и неофициальные свидетельства и факты, но и рассматривают это событие как ***ключевое звено*** в цепи других аналогичных провокационных событий прошлого – от убийства Джона Кеннеди, Уотергейта, Ирангейта, крушение рейса KAL 007, подрыва Всемирного Торгового Центра в 1993 г. и др.

Чтобы помочь читателю глубже «окунуться» в непростые проблемы идентификации исполнителей кибератак, здесь мы вынуждены перейти от терминов «простого» языка к более сложным понятиям. Начнем с того, что есть такое понятие – ***атрибуция*** (от латин. ***Attribution*** – приписывание) – это психологический термин, обозначающий механизм объяснения причин поведения другого человека. В более широком смысле оно означает ***приписывание*** социальным объектам (человеку, группе людей) характеристик, «не представленных в поле восприятия». Например, иногда информация, которую могут дать человеку наблюдения, недостаточна для адекватного взаимодействия с социальным окружением и нуждается в «достраивании» (домысливании). Так вот, основным методом такого «достраивания-домысливания» непосредственно воспринимаемой информации и является атрибуция.

До недавнего времени американские и английские спецслужбы широко использовали этот метод при расследовании «киберинцидентов» (например, Дэвид А. Уиллер и Грегори Н. Ларсен «Методы атрибуции кибератак». – Виржиния: Институт оборонного анализа, 2005). Но как можно увидеть из текста Стратегии кибербезопасности США (находится в открытом доступе http://d-russia.ru/wp-

content/uploads/2019/01/National-Cyber-Strategy_USA_2018.pdf), говоря простым языком, американцы решили особо «не заморачиваться» и «мочить» всех, кто по их «обструктивным» предположениям\домысливаниям может быть их исполнителем. Здесь можно привести аналогию с известным «английским» термином, введенным в оборот Терезой Мей *«highly likely»* («весьма вероятно»).

Тем не менее чтобы перейти непосредственно к рассмотрению темы идентификации исполнителей кибератак, следует отметить следующее. Хотя продекларированный американский принцип «мочить всех» будет главным, тем не менее никто не снимает с повестки дня эту проблему. Более того, она становится одной из главных «головных болей» атакованной стороны. Ведь в случае кражи секретной (или особо секретной) информации, «потерпевшей» стороне небезразлично, кто конкретно завладеет этой информацией, и здесь дело не в «возмездии» – именно от успешного решения этой задачи будет зависеть структура и содержание системы (комплекса) «защитных мероприятий». Цель подобных мероприятий – избежать максимального урона (материального, финансового, имиджевого, военного, политического и др.), от приобретения противником секретной информации и срочно разработать конкретные меры по «залатыванию» обнаруженной «дыры» в защитных барьерах.

Поэтому, как мы уже показали в разд. 1.5 и 1.6 предыдущей главы, выявление исполнителей кибератак сегодня стало очень прибыльным высокоинтеллектуальным бизнесом.

2.3.2. Зачем нужна идентификация источника кибератаки

По заказу НАТО уже несколько лет ведется работа над второй редакцией известного специалистам по международному праву так называемого Таллинского руководства по применению международного права при ведении кибервойн, еще в первой версии которого ***обосновывалась возможность физического ответа на кибернападение***. Очевидно, что в такой ситуации как никогда важна правильная идентификация источника киберугроз. Ошибочная идентификация может привести к развязыванию войны (локальной, региональной или глобальной) или, наоборот, привести к тому, что будет упущено время, необходимое для подготовки к отражению агрессии. Неспособность установить истинного виновника и тем более заказчиков, не позволит в полной мере задействовать имеющиеся в распоряжении каждого государства дипломатические, политические и юридические рычаги.

Поэтому идентификация нужна не только для того, чтобы понять, кто действует против нас, но и чтобы выстроить оборонительную стратегию и спланировать защитные действия. Один вариант, если мы имеем дело с нарушителем, за которым стоит государство; если же угроза реализована негосударственным *актором*, то и ответные действия должны быть другие. Не на техническом уровне – тут механизмы защиты будут практически одинаковыми (если не рассматривать возможность бомбардировок в ответ на сканирование сети), а на дипломатическом и правовом, и именно от идентификации будет зависеть набор шагов, которые предпримет государство.

Говоря об идентификации, надо заранее понять, насколько точно мы хотим ответить на вопрос *кто нас атакует,* до какого уровня детализации дойти. Как

было показано в нашей книге «Кибероружие и кибербезопасность. О сложных вещах простыми словами» Таллинское руководство не особо глубоко погружается в детали и просто ***ищет основания для применения традиционных вооружений*** против кибернападений, поэтому атрибуция в нем ограничивается определением государства, с территории которого фиксируется кибератака.

Идентификация узла, с которого осуществляется воздействие в киберпространстве, необходима, чтобы понять, принадлежит этот узел частному лицу или организации, какой интернет-провайдер выделил IP-адреса для данного узла (возможно, этот провайдер ранее был замечен и в других кибератаках), физическое местоположение данного узла (которое зачастую можно определить), настройки узла, вплоть до используемой операционной системы и приложений, по которым можно попробовать определить языковую или национальную принадлежность атакующего, и т.д.

Идеально, если в рамках этой работы можно будет сделать ***вывод о*** мотивах совершаемых действий. Однако определение мотивации – это уже «высший пилотаж» в области идентификации спецопераций в киберпространстве и только техническими средствами решить эту задачу невозможно.

Сегодня в мире существует целый ряд компаний, которые специализируются только в этой области. Можно привести отдельные примеры проведенных ими относительно успешных операций по идентификации:

- *Cylance*, которая изучала кампанию иранских хакеров *Cleaver (Нож мясника)*;
- *Partners*, которая раскрыла операцию *Newscaster (Телекомментатор),* также исходившую из Ирана;
- *Лаборатория Касперского*, которая раскрыла кампании *Маска* и *Красный октябрь*;
- *Group-IB*, нашедшая след *Исламского государства* в атаках на многие российские организации;
- *BAE Systems*, исследовавшая атаки на украинские компьютеры и нашедшая на них *русские* отпечатки;
- *Check Point*, раскрывшая ливанскую хакерскую группу *Volatile Cedar (Летучий кедр)*;
- *Taia Global*, которая вопреки распространенному мнению, что компанию *Sony* взломали хакеры из Северной Кореи, *доказала,* что *Sony* все-таки атаковали из России.

Надо сказать, что ***кибератаки военного назначения сегодня превратилась в инструмент геополитической борьбы***. Что может быть проще, чем обвинить то или иное государство в агрессии только на том основании, что с его территории зафиксирована кибератака. И, как мы неоднократно наблюдали за последнее время, отдельные страны и блоки стран активно используют этот прием.

Желание связать конкретную атаку с конкретным государством, не разбираясь в реальных источниках и причинах, вполне объяснимо – это удобный прием в геополитической борьбе, особенно если нужно быстро создать образ врага.

Отдельно стоит упомянуть, что идентификация источника в сложной атаке, проходящей через несколько государственных границ и континентов, требует активного взаимодействия представителей государств, не только находящихся

в разных юрисдикциях, но иногда и агрессивно, даже враждебно по отношению друг к другу настроенных. Можно ли быть уверенным, что такое сотрудничество будет налажено? Далеко не всегда, но можно.

Например, как было отмечено в нашей книге «Кибероружие и кибербезопасность. О сложных вещах простыми словами», на конференции *Positive Hack Days* в Москве представители ФСБ заявили [18], что в настоящий момент большая часть хакерской активности, направленной против России, идет с территории Украины, но нормально взаимодействовать с украинскими спецслужбами не удается по вполне понятным причинам. Хотя иногда наблюдается и обратная картина. Например, во время подготовки и проведения зимних Олимпийских игр в Сочи *американские и российские спецслужбы достаточно активно взаимодействовали в рамках* обеспечения безопасности игр. И это несмотря на уже произошедшее охлаждение дипломатических отношений, заморозку отдельных контактов и приостановление работы ряда рабочих групп.

2.3.3. Основные проблемы решения задачи идентификации источника кибератаки

Здесь существует множество проблем – от чисто «технических», методологических, организационных до юридических и морально-этических. Технические сложности заключаются в невозможности простого определения источника атак в киберпространстве, причем независимо от формы их реализации – в виде DDoS-атак, путем проникновения через защитные экраны, в виде рассылок вредоносного кода через электронную почту или путем заражения сайтов и флешек, через которые вредоносное ПО попадает во внутреннюю сеть предприятия.

В 1960-1970-е гг., когда создавались протоколы, положившие начало современному Интернету, никто не задумывался о необходимости однозначной идентификации всей цепочки передачи пакетов данных из точки А в точку Б. Более того, *сама по себе технология работы Интернета подразумевает децентрализацию и распределенность*. И то, что устраивало всех последние 40 лет, сейчас стало играть с нами дурную шутку. Как определить реального автора пришедшего мне на компьютер сетевого пакета, если технически возможно изменить адрес отправителя? Все известные версии протокола IP в принципе не подразумевают однозначной идентификации и аутентификации инициатора соединения (хотя разговоры об интернет-паспортах и идентификации всех, кто входит в Интернет, ведутся давно).

Но отсутствие в имеющейся на момент выхода книги версии протокола IPv4 необходимых атрибутов для определения местоположения источника атаки – далеко не единственное препятствие. Никто ведь не может помешать злоумышленнику, желающему скрыть свое истинное местоположение, использовать любой имеющийся в Интернете прокси-сервер (сервер-посредник) или анонимайзер. В случае реализации атаки через них мы увидим в качестве адреса источника атаки *не реальный адрес злоумышленника, а адрес сервера-посредника*. Как быть в таком случае? А ведь такие сервера во множестве разбросаны по разным национальным сегментам Интернета. Находясь в Пекине, атакующий может реализовать атаку через посредника в Пекине, Москве, Сеуле или Гонолулу.

Ситуация усугубляется тем, что злоумышленник может арендовать *специальные сервера* (так называемый abuse-устойчивый хостинг), которые будут целенаправленно скрывать истинный адрес злоумышленника. И таких промежуточных серверов может быть много – 5, 10, 100. В такой ситуации атака обладает *динамически меняющимися пространственными характеристиками*, что коренным образом отличает ее от обычных наступательных вооружений. Может ли ядерная боеголовка динамически менять свое местоположение? Да, но очень медленно, если возить ее на специальном автотранспорте или поезде. Но и в этом случае ее географические координаты ограничены границами одного государства, в крайнем случае блока. *Для кибератаки поменять за несколько минут или даже секунд географическую привязку и числиться на разных континентах – в порядке вещей.*

Аналогичная ситуация возникает и если подняться выше по так называемому *стеку интернет-протоколов* и посмотреть на электронную почту, которая может содержать угрозы или реальный вредоносный код. Идентифицировать настоящего отправителя почты, если он того не желает, практически невозможно. Для этого надо пройти по цепочке всех узлов, через которые проходило почтовое сообщение и которые могут находиться в разных странах и юрисдикциях.

Отдельный вопрос с файлами и вредоносным программным обеспечением. У них нет никакой «печати» и, как правило, не стоит подпись автора, который желал бы оставить свой след в истории. Поэтому исследователям приходится просматривать огромные объемы информации в поисках *зерен правды,* позволяющих *с определенной долей вероятности* определиться с источником атаки. Например, в рамках расследования операции *Нож мясника* вышеупомянутая компания *Cylance* собрала и изучила свыше 8 Гб данных, 80 000 файлов, журналы регистрации на узлах жертв и т. п. И только после этого она смогла заявить об «иранском следе», и то с оговорками. Однако технический анализ так и не смог дать ответ на вопрос, стояло за этой операцией *государство* или это была *частная инициатива.*

2.3.4. Основные индикаторы (признаки), используемые при определении источников кибератак

Как уже было указано выше, такие компании, как *Group-IB, Лаборатория Касперского, Cisco, Cylance, Taia* и другие, проводят свои расследования, используя в качестве доказательств следующие индикаторы (признаки):

Место регистрации IP-адресов и доменов, участвующих в атаке или предоставляющих инфраструктуру для реализации атаки. При этом анализируется не только страна регистрации, но и сопутствующая информация, которая может быть получена с помощью сервиса WHOIS: ФИО владельца домена или IP-адреса, его контакты. Все это позволяет при превышении определенного порогового значения сделать вывод о стране, которая *стоит за кибернападением.* Если же злоумышленник не очень квалифицированный, можно идентифицировать и физическое место расположения источника атаки.

Трассировка атаки до ее источника или хотя бы локализация области, в которой источник находится. Такой функционал есть у многих маршрутизаторов, на которых построен Интернет. Помимо механизма *Traceback,* использующегося на сетевом

оборудовании, для идентификации злоумышленников могут быть использованы фильтрация трафика на интерфейсах маршрутизатора (ingress filtering), протокол ICMP для возврата отброшенного на жертву трафика обратно его инициатору. Например, в случае шпионской кампании *Лунный лабиринт (Moonlight Maze*[10]*),* направленной против ВПК США, НАСА и ряда американских государственных структур, отследить организаторов удалось именно путем анализа обратного маршрута до серверов, зарегистрированных в России (правда, связь с государственными структурами так и не была установлена).

Временные параметры. Как показали ранее приведенные примеры, нередко исследователи анализируют время создания вредоносного кода, время начала операции в киберпространстве или время наибольшей активности. Пусть и с оговорками, но эта информация может служить основой дальнейшего анализа. И хотя она не укажет на конкретного нарушителя, она позволит сузить число стран, которые могли бы быть причастны к анализируемой ситуации.

Анализ программного кода, в котором могут быть найдены комментарии, ссылки на сайты, домены, IP-адреса, которые участвуют в атаке. Анализ функциональности программного кода позволяет сузить число возможных нарушителей. Например, анализ кода *Stuxnet* показал, что для его создания надо было не только знать, как работают центрифуги IR-1 в Натанзе, но и иметь стенд для проверки работоспособности вредоносного кода, который позже вывел из строя большое количество центрифуг по обогащению урана. Но многие ли *акторы* способны приобрести центрифуги для тестирования? Это позволило существенно снизить число возможных нападавших, а дополнительные сведения позволили даже назвать государства, которые стояли за разработкой *Stuxnet*, – США и Израиль.

Помимо изучения фрагментов кода, отдельные исследователи пытаются даже ***изучать почерк программистов и определять по нему школу программирования****:* американская, русская, китайская и т. п.

С анализом почерка тесно связана и лингвистика, а точнее ***стилометрия****,* которая ***позволяет определить стилистику языка в тех же самых комментариях или сопутствующих текстах***. Известно, что то, в какой стране родился человек, в какой культуре рос, в какой языковой среде воспитывался, определяет его стиль письма, который можно выделить и зафиксировать. Например, выросший в России или Советском Союзе человек, позже уехавший в Великобританию или США, никогда не будет говорить на языке так же, как коренной англичанин или американец. Эти различия позволили, например, специалистам компании *Taia Global* сделать вывод о том, что за атаками на *Sony* стоят не северокорейские, а русские хакеры. Аналогично эксперты *Лаборатории Касперского* предположили, что за шпионской кампанией *Маска* стоят испаноговорящие хакеры. Причиной такого вывода послужило использование в коде испанских слов и сленга, которые никогда не используется англоговорящей аудиторией.

Обманные системы или honepot/honeynet – популярный в свое время инструмент, интерес к которому со временем поугас, а сейчас возвращается вновь. Идея проста: в сети запускается фальшивый, подставной узел, который злоумышленник атакует, оставляя следы своей несанкционированной активности, – вот ее-то и изучают эксперты.

Еще один метод – ***оперативная разработка***. Он мало чем отличается от того, что мы знаем из боевиков или детективов. Внедренные агенты, *стукачи, сочувствующие* и другие источники информации позволяют идентифицировать или хотя бы сузить спектр возможных акторов, стоящих за той или иной атакой. Хороший пример – Эдвард Сноуден, который успел рассказать немало интересного о деятельности спецслужб, в которых ему довелось служить.

Анализ активности на форумах и в социальных сетях. Именно так в 2007 г. была выяснена причастность молодежного движения *Наши* к атакам на ряд эстонских ресурсов. Однако связь *Наших* с российскими властными структурами в данном конфликте так и не была подтверждена. Аналогичным образом после публикации ролика на *YouTube* иранской хакерской группировки *Izz ad-Din al-Qassam Cyber Fighters* была *доказана* роль иранских хакеров (но не самого государства) в атаках на американские банки. Наконец, Сирийская электронная армия регулярно берет на себя ответственнось за атаки на отдельные американские ресурсы. Например, именно они заявили о взломе учетной записи в *Твиттере агентства Assocaited Press*, в котором написали о взрыве в Белом Доме и ранении Барака Обамы. Анализ активности хакеров и оперативная разработка – единственные методы определения мотивов кибератаки. Ни анализ IP-адресов, ни лингвистика не дают возможности ответить на вопрос *почему,* ограничиваясь только ответом на вопрос *кто*.

В отдельных случаях *автора можно идентифицировать постфактум по его действиям*. Речь идет не только о том, что он осознанно или случайно делится фактом своего участия в атаке в социальных сетях. Например, в случае вторжения в интернет-банк, кражи денег и перевода их на подставные или реальные счета, наблюдая за владельцем счета, можно выйти и на тех, кто стоит за ним или кто его нанял. Также украденная информация может появиться на аукционах и биржах, публичных и закрытых. Дальше следователи могут вступить в переговоры с продавцом и провести его атрибуцию или получить важную информацию для дальнейшей атрибуции кибернападения.

Из всего вышесказанного следует, что универсального и 100-процентного метода не существует. Более того, далеко не всегда техническими методами можно ограничиться. Например, когда в 2012 г. стало известно об атаке вредоносного кода *Gauss* на ливанские банки, многие эксперты задавались вопросом: *а зачем это было нужно?* Неужели нет более лакомых кусков, чем ливанские банки? И поскольку технические методы не помогли провести правильную атрибуцию, пришлось использовать косвенные признаки. Например, по анализу функций кода *Gauss* исследователи предположили, что он направлен на изучение счетов организации *Хезболла,* которая таким образом отмывала деньги, что и интересовало тех, кто стоял за атакой на финансовые институты Ливана. А учитывая, что *Хезболла* признана террористической организацией в ограниченном числе стран (в частности, в США и Израиле), спектр возможных инициаторов был сужен до пары государств.

Из американской разведки вышел широко известный специалистам по безопасности и используемый в расследовании киберпреступлений термин *OSINT (open source intelligence)*, т. е. поиск, сбор и анализ информации, полученной из открытых источников. Сегодня без активного развития и использования инструментов *OSINT* сложно эффективно заниматься идентификацией спецопераций в кибер-

пространстве, а эта техника требует высокой квалификации лиц, которые участвуют в определении источника кибернападения. Это могут быть как сотрудники служб информационной безопасности государственных органов и критически важных объектов, так и представители правоохранительных и силовых структур, уполномоченных проводить оперативно-розыскную деятельность в киберпространстве.

Так или иначе, но одним из основных моментов при решении задач идентификации является высокий уровень квалификации «охотников» – специалистов по кибербезопасности, киберразведке, киберконтрразведке. Далее в этой книге мы сформулируем основные требования к уровню подготовки таких специалистов, методикам их обучения и тренировки.

Литература к главе 2

1. Белоус А.И., Солодуха В.А. Кибероружие и кибербезопасность. О сложных вещах простыми словами. – М., Вологда: Инфра-Инженерия, 2020.
2. Белоус А.И., Солодуха В.А., Шведов С.В. Программные и аппаратные трояны – Способы внедрения и методы противодействия. Первая техническая энциклопедия. В 2 кн. – Т. 1. – М.: Техносфера, 2018. – 688 с.
3. Журнал «Огонек». – 2018. – № 41. – 29 октября. – С. 5.
4. Фалеев М.И., Сардановский С.Ю. Вопросы кибербезопасности в современной государственной политике в области национальной безопасности. – Технологии гражданской безопасности, 2016
5. Старовойтов А.В. Кибербезопасность как актуальная проблема современности // Информация и связь. – 2011. – № 6. – С. 4–7.
6. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (ч. 2) // Вопросы кибербезопасности. – 2014. – № 1 (2). – С. 5–12.
7. Марков Г.А. Вопросы физической безопасности информации // Вопросы кибер-безопасности. – 2015. № 4 (12). – С. 70–76.
8. Petrenko S.A. Model Cyber Threats by Analysis of DARPA Innovations.
9. Клабуков И.Д., Алехин М.Д., Нехина А.А. Исследовательская программа DARPA на 2015 год. – М., 2013. – 102 с.
10. Клабуков И.Д., Алехин М.Д., Мусиенко С.В. Сумма технологий национальной безопасности и развития. – М., 2013. – 110 с.
11. Официальный сайт агентства по перспективным оборонным научно-исследовательским разработкам Defense Advanced Research Projects Agency, DARPA. URL: www.darpa.mil (дата обращения: 12.01.2015).
12. Kellerman T. Cyber-threat proliferation: Today's truly pervasive global epidemic // Security Privacy, IEEE. – 2010. – Vol. 8. – No. 3. – P. 70–73.
13. 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.
14. 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. – P. 137–140.

15. 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. – P. 9–14.
16. 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. – P. 219–226.
17. 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. – P. 443–446. URL: http://dx.doi.org/10.1109/ASE.2008.69
18. Стратегия национальной кибербезопасности Соединенных Штатов Америки. URL: http://d-russia.ru/wp-content/uploads/2019/01/National-Cyber-Strategy_USA_2018.pdf
19. Сырков Б. Сноуден – самый опасный человек в мире. – М: Алгоритм, 2016. – 432 с.
20. https://tvnews.by/analitics/15076-otchet-evrosojuza-svjaz-pjatogo-pokolenija-neset-v-sebe-massu-kiberugroz.html