УДК 004.7

М. И. Авилов
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Система мониторинга компьютерной сети и определение ее критериев при проведении киберучений

Рассматривается вопрос задействования системы сетевого мониторинга при проведении киберучений, а также предлагаются критерии выбора или проектирования системы сетевого мониторинга. Рассматриваются такие подходы к мониторингу информационно-вычислительных сетей, как проактивный и реактивный, а также объясняется, для чего каждый подход необходим. Рассматриваются способы опроса и сбора данных с сетевых узлов информационно-вычислительной сети киберучений. Дается описание возможных последствий при отказе от задействования системы сетевого мониторинга, в результате чего контроль за информационно-вычислительной сетью, которая заранее разворачивается для проведения киберучений, может быть значительно осложнен. Выявление же причин возникающих сбоев без системы сетевого мониторинга и мест, где эти сбои происходят, может занять продолжительное время, что в свою очередь негативно скажется на процессе проведения киберучения.

Система мониторинга, информационно-вычислительная сеть, киберучения, проактивный и реактивный мониторинг

В последнее время можно все чаще встретить информацию о проведении различных киберучений. Например, Locked Shields-2018, Кибер-Антитеррор-2016, Cyber Europe-2014, II Кубок CTF и др. Для понимания сути этих мероприятий необходимо уточнить термины «киберучение», «киберпространство» и «информационное пространство».

В Российской Федерации используется более «широкий» термин – *информационное пространство*, под которым понимается «сфера деятельности, связанная с созданием, преобразованием и использованием информации, включая индивидуальное и общественное сознание, информационно-телекоммуникационную инфраструктуру и собственно информацию» [1].

Под *киберпространством* (этот термин используется в Соединенных Штатах Америки) понимают «глобальное пространство в цифровой среде, состоящее из взаимозависимых сетей информационно-коммуникационных инфраструктур, в том числе Интернета, сетей связи, компьютерных сетей и встраиваемых процессоров и контроллеров» [2].

Группа же экспертов из института «Запад–Восток» и Института проблем информационной безопасности (ИПИБ) МГУ им. М. В. Ломоносова определила киберпространство как «электронную (включая фотоэлектронные и пр.) среду, в (посредством) которой информация создается, передается, принимается, хранится, обрабатывается и уничтожается» [2].

Также необходимо иметь в виду, что «кибер» происходит от греческого слова κυβερνητικός и означает искусство управления. «Кибер» задействован в термине «кибернетика», который был введен в книге Норберта Винера «Кибернетика, или Управление и связь в животном и машине». Автор данной книги применял этот термин в контексте контроля сложных систем. Впервые же термин «кибернетика» ввел Ампер в своем труде «Опыт о философии наук, или аналитическое изложение естественной классификации всех человеческих знаний».

Что же касается «пространства» в термине «киберпространство», то здесь подразумевается наличие определенного измерения. Также киберпространство рядом людей приравнивается к суше, водному и воздушному пространству, а также космосу. Однако если эти среды являются естественными, то киберпространство – искусственно создано человеком [2].

В настоящее время термин «киберпространство» полезен тем, что может быть задействован для определения отличного от физического или виртуального мира, созданного Интернетом и различными электронными средствами связи.

Под *киберучениями* понимаются специальные мероприятия, которые представляют собой решения задач информационного противоборства непосредственно на практике. Например, такие задачи, как предупреждения компьютерных атак, нейтрализация последствий атак на сети и системы критически важных объектов. Организацию и проведение таких учений стараются осуществить в условиях, максимально приближенных к реальным. Основными целями и задачами киберучений являются приобретение новых, а также закрепление старых навыков противоборства в киберпространстве, кооперация соответствующих подразделений для осуществления оборонительных и наступательных операций, отработка тактических и стратегических сценариев развития возможных, возникающих в процессе противоборства, конфликтов в киберпространстве [3].

Необходимость проведения киберучений с каждым годом только возрастает, а с учетом несовершенства известных моделей, методов и средств обнаружения, предупреждения и нейтрализации последствий компьютерных атак ввиду того, что с каждым разом атаки усложняются, используя все более новые технологии, проведение подобных учений является одним из важных мероприятий по поддержанию информационной безопасности. Например, в США с 2006 г. проводятся крупномасштабные киберучения «Cyber Storm» [4].

Сами же киберучения должны проводиться в соответствии с требованиями планирующих документов, в отдельных случаях – по указаниям соответствующих должностных лиц. Основными условиями подготовки и проведения киберучений являются [5]:

– всесторонний учет характера возможных последствий информационно-технических воздействий атакующей стороны;

– практический опыт нейтрализации групповых и массовых кибератак.

Также немаловажным является и то, что при проведении киберучений необходим мониторинг используемого сетевого оборудования, как проактивный, так и реактивный.

Проактивный мониторинг в данном случае необходим для того, чтобы собирать данные как о доступности сетевых устройств, так и о различных действиях атакующей и защищающейся сторон при проведении киберучений. Данный мониторинг необходим для дальнейшего анализа и выработки методов проведения учений в дальнейшем.

Реактивный мониторинг в свою очередь необходим для поддержания как непосредственно самой сетевой среды по проведению киберучений, так и для возможного внесения коррективов в виде дополнительных, заранее заготовленных, заданий в процессе проведения данного мероприятия.

Это означает, что становится актуальным подбор или разработка системы (систем) мониторинга. Однако в рамках киберучений при выборе или разработке системы мониторинга за состоянием сетевых устройств и сетевых действий участников необходимо изначально определиться с критериями для системы мониторинга.

При проактивном мониторинге необходимо учитывать:

– мониторинг ресурсов вычислительных устройств, например нагрузку на центральный процессор, оперативную память и другие вычислительные ресурсы сетевого устройства;

– мониторинг файлов журналирования, например мониторинг объемов и видов запросов (запросы к базе данных, запросы к веб-службам и др.);

– мониторинг авторизации и аутентификации пользователей на сетевых узлах, например на серверах, маршрутизаторах, коммутаторах, которые задействованы в киберучениях;

– мониторинг доступности сетевых узлов, например при помощи команды ping с разрешенного устройства.

При реактивном мониторинге необходимо учитывать:

– мониторинг прохождения пороговых значений, преодолев которые осуществляется реакция по заранее написанному сценарию. Например, если был осуществлен выход температурных показателей за пределы, установленные как «нормальные», то такому устройству может быть послана команда выключения;

– мониторинг критически важных возможных ситуаций в среде проведения киберучений, при наступлении которых произойдет воздействие по заранее написанному сценарию (например, переход на дополнительное резервное электропитание);

– мониторинг выполнения прописанных заранее заданий, выполнив которые будет осуществлен сценарий с «непредвиденными событиями». Например, получив атакующей командой доступ к коммутатору, система мониторинга выполнит сценарий, по которому через некоторое время несохраненная конфигурация будет потеряна посредством сброса к первоначальному сконфигурированному виду, если атакующие не заметят такой защиты;

– мониторинг выполнения заранее установленных правил при проведении киберучений. Например, отслеживание использования запрещенных устройств и автоматическое блокирование таковых в рамках проведения учений.

Исходя из перечисленных требований, предлагаются следующие критерии:

– оптимальность нагрузки на сетевой канал. Объемы данных, передаваемых по сети, должны минимально влиять на скорость передачи данных между сетевыми хостами, участвующими в киберучениях;

– время готовности системы. При выходе из строя одного из модулей системы сама система должна продолжать работу и при восстановлении модуля в режиме реального времени его подключить;

– оптимальность нагрузки на вычислительные ресурсы сетевого узла. Агенты системы мониторинга или другие способы сбора и передачи информации менеджеру системы мониторинга не должны загружать вычислительные ресурсы хоста, так как при большой нагрузке хосты могут некорректно работать, тем самым мешая проведению киберучений;

– надежность передачи данных. Передача данных по сети только по протоколу UDP, т. е. без установления соединения, упорядочения и проверки целостности данных, не гарантирует получения всех необходимых данных. Поэтому помимо SNMP-трафика, который идет при помощи UDP, необходимо задействовать дополнительные инструменты, работающие по TCP (например, дополнительное программное обеспечение, которое задействует TCP);

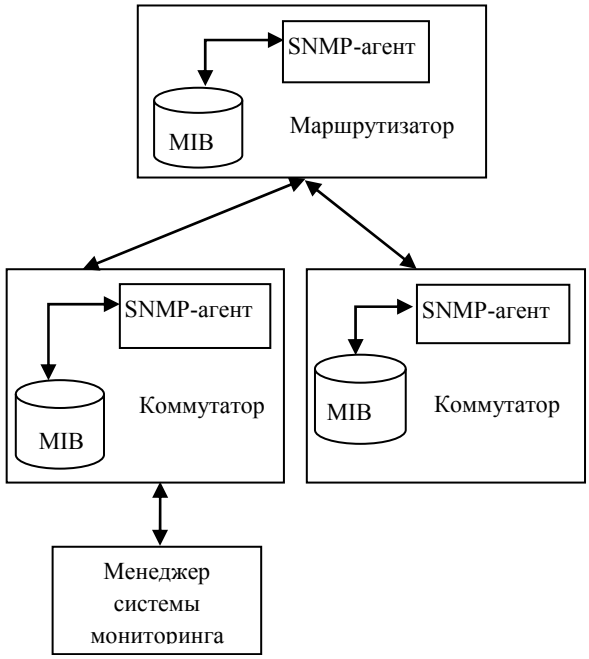
– масштабируемость. При необходимости систему мониторинга можно дополнить новыми модулями, которые будут снимать нагрузку с другого модуля либо выполнять отдельные вычислительные операции.

Сами же данные могут собираться «зеркалированием» трафика на моделях активного сетевого оборудования [6]. Помимо «зеркалирования» можно получать информацию при помощи SNMP (Simple Network Management Protocol), RMON (Remote Monitoring). Известным и распространенным протоколом управления сетями является протокол SNMP, где информация о состоянии объектов хранится в MIB (Management Information Base). Пример работы по SNMP показан на рисунке. Компьютерная сеть, которая задействует протокол SNMP, содержит 3 основных компонента [7]:

1. SNMP-менеджер или менеджер системы мониторинга, который является программным обеспечением и устанавливается на персональный компьютер администратора сети или же может находиться на сервере с самой системой мониторинга.

2. SNMP-агент – это программное обеспечение, запущенное на узле, за которым осуществляется мониторинг. Агент имеет возможность управлять информацией и переводить ее в специфичную для SNMP форму.

3. NMS (Network Maganement System) – программное обеспечение, которое взаимодействует с менеджерами для поддержки общей структуры данных, показывающей состояние сети.



При использовании RMON объекты в MIB содержат дополнительные счетчики ошибок в пакетах, более гибкие средства анализа трендов и статистики, мощные средства фильтрации для захвата и анализа отдельных пакетов, а также сложные условия установления сигналов предупреждения. Интеллектуальность агентов RMON MIB выше, чем агентов MIB-I и -II, что позволяет им выполнять значительную часть работы, которую ранее выполняли менеджеры [8].

Объекты RMON в MIB располагаются в следующих группах [9]:

– ethernet statistics. Данная группа содержит статистику, измеренную специальным датчиком для каждого контролируемого устройства в сети;

Преимущества	Недостатки
Возможность отслеживать состояния сетевых узлов	Необходимы дополнительные ресурсы сетевой вычислительной техники для работы системы мониторинга
Возможность сбора информации о действиях участников учений для выработки новых методов проведения киберучений	Дополнительные финансовые расходы на оборудование, приобретение лицензий, возможно, на разработку и обслуживание необходимой системы мониторинга
Возможность осуществления реакции по заранее спланированному сценарию (реактивный мониторинг)	Требуются квалифицированные специалисты для инсталляции, настройки или разработки системы мониторинга
Возможность контролировать выполнение заранее установленных правил	В процессе эксплуатации возрастет нагрузка на каналы передачи данных информационно-вычислительной сети
Возможность вносить необходимые коррективы в процесс проведения киберучений в режиме реального времени	–

– history control. Группа, которая предназначена для контроля периодичности статистической выборки данных из компьютерных сетей;

– ethernet history. В эту группу записываются периодические статистические выборки из сети Ethernet и сохраняются для их последующего поиска;

– alarm. Данная группа периодически принимает статистические отчеты от датчиков и сравнивает их с ранее настроенными пороговыми значениями;

– host. Группа содержит статистику, связанную с каждым узлом, обнаруженным в сети. В ней сохраняются данные MAC-адресов источника и получателя, которые видны в сетевых пакетах;

– hostTopN. Группа, позволяющая упорядочить списки основываясь на пиковых значениях трафика группы элементов;

– matrix. Группа матриц, хранящая статистику трафика между парами узлов. Когда устройство обнаруживает новую передачу, то в группе создается новая запись;

– filter. Данная группа позволяет отфильтровать необходимый трафик по определенным критериям;

– packet capture. Данная группа предназначена для захвата пакетов в канале;

– event. Данная группа предназначена для управления генерацией и уведомления о событиях, связанных с контролируемым устройством.

Используя SNMP, RMON можно отслеживать необходимые события в информационно-вычислительной сети в процессе проведения мероприятий по киберучениям и на этой основе создавать соответствующие политики мониторинга для каждого компонента данной сети [10].

Если же не осуществлять мониторинг при проведении киберучений, то появляются следующие проблемы:

– становится довольно сложно отслеживать действия участников, что в свою очередь затрудняет в дальнейшем выработку методик по защите критически важных объектов информационной инфраструктуры;

– при возникновений сбоев в предоставленной сетевой среде для проведения киберучений выявление их причин и мест, где они происходят, может занять большее время, чем при использовании системы мониторинга;

– контролировать выполнение заранее установленных правил при проведении учений также становится довольно затруднительно;

– нет отслеживания пороговых показателей на сетевых узлах, где выход за установленные заранее пороговые показатели может привести как к сбоям в работе сетевой среды, так и к полной непригодности оборудования для эксплуатации.

В таблице представлены преимущества и недостатки использования сетевой системы мониторинга.

Из изложенного следует, что задействование системы мониторинга при проведении киберучений значительно упростит сбор необходимой информации для дальнейшего анализа и выработки методик защиты от деструктивных воздействий атак как на определенные информационно-вычислительные системы, так и на сами системы мониторинга информационно-вычислительной среды киберучний. Приведенные преимущества и недостатки отражают аспекты использования системы мониторинга. Предложенные в статье критерии выбора или проектирования системы мо-

ниторинга при проведении киберучений позволяют заранее определиться с тем, на что необходимо обращать внимание, а задействование проактивного и реактивного мониторинга позволит упростить как отслеживание состояния информационно-вычислительной среды, так и выполнение установленных правил киберучений.

СПИСОК ЛИТЕРАТУРЫ

1. Словарь терминов и определений в области информационной безопасности. 2-е изд., доп. и перераб. / Военная акад. Генерального Штаба Вооруженных сил РФ. Научно-исследовательский центр информационной безопасности. М., 2008. С. 40.

2. Двусторонний проект Россия–США по кибербезопасности. Основы критически важной терминологии. 1-е изд. / под ред. К. Ф. Раушера, В. В. Ященко. 2011. С. 12. URL: http://www.iisi.msu.ru/UserFiles/File/Terminology%20IISI%20EWI/Russia-U%20S%20%20bilateral%20on%20terminology%20RUS.pdf (дата обращения 9.10.18).

3. Петренко С. А., Ступин Д. Д. Национальная система раннего предупреждения о компьютерном нападении. СПб.: Издательский Дом «Афина», 2017. С. 27.

4. Петренко А. А., Петренко С. А. НИОКР Агентства DARPA в области кибербезопасности // Вопросы кибербезопасности. 2015. № 4 (12). С. 2–22.

5. Петренко А. А., Петренко С. А. Киберучения: методические рекомендации ENISA // Вопросы кибербезопасности. 2015. № 3 (11). С. 8.

6. Петренко С. А. Метод обнаружения несанкционированного копирования Ethernet-трафика кибероъектов // Тр. Ин-та системного анализа Российской акад. наук. 2009. Т. 41. С. 158–166.

7. Шохина К. С., Иванова М. Н. Возможности протокола SNMP // Науч. сб. статей междунар. науч.-практ. конф.: в 8 ч. В мире науки и инноваций. 2016. С. 206–208.

8. Савченко А. С. Системный анализ протоколов управления крупной корпоративной сетью // Проблемы информатизации и управления. Национальный авиационный ун-т. 2012. Т. 3, № 39. С. 135–142.

9. Waldbusser S. Remote Network Monitoring Management Information Base // RFC-1757, February 1995. P. 5–7. URL: https://tools.ietf.org/html/rfc1757 (дата обращения 9.10.18).

10. Петренко С. А., Курбатов В. А. Лучшие практики создания нормативных документов по кибербезопасности в компании // Тр. Ин-та системного анализа Российской акад. наук. 2006. Т. 27. С. 177–233.

M. I. Avilov
Saint Petersburg Electrotechnical University «LETI»

ROLE NETWORK MONITORING SYSTEM IN THE TECHNICAL CYBER DEFENCE EXERCISE

The question of using the network monitoring system during cyber exercises is considered, as well as the criteria by which the choice or design of the network monitoring system can be carried out. We consider such approaches to the monitoring of information and computing networks as proactive and reactive, and explains why each approach is necessary. The article considers the methods of survey and data collection from the network nodes of the information and computer network of cybersecurity. Given the possible consequences in case of refusal from the start of the network monitoring system, resulting in control over the data processing network, which is in advance of razorace cates for holding cimarusti may be significantly complicated. Identification of the causes of failures, without a network monitoring system, and the places where these failures occur, can take a long time, which in turn will adversely affect the process of cyber-learning.

Network monitoring system, computer network, technical cyber defence exercise, proactive and reactive monitoring