УДК 004.056 Вестник УрФО № 4(34) / 2019, с. 22–29

Гибилинда Р. В., Фартушный А. В.

DOI: 10.14529/secur190403

ПРОГРАММНЫЙ ИНСТРУМЕНТАРИЙ ГЕНЕРАЦИИ КОМПЛЕКСНЫХ КОМПЬЮТЕРНЫХ АТАК ПРИ ИМИТАЦИОННОМ ТЕСТИРОВАНИИ СИСТЕМ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье представлены модели элементарной и комплексной компьютерных атак, модели события и инцидента информационной безопасности (ИБ), а также описан программный инструментарий для проведения имитационного тестирования систем управления инцидентами информационной безопасности (SIEM-системы), реализованный в виде генератора комплексных компьютерных атак. Он предназначен для осуществления целенаправленного атакующего воздействия на узлы сетевой инфраструктуры, контролируемой SIEM-системой. Комплексные компьютерные атаки, созданные в виде сетевого трафика, описываются сценарием. Его выполнение позволяет оценить возможности SIEM по определению широкого спектра угроз ИБ — воздействиям на файлы, установки утилит удаленного администрирования, изменениям параметров конфигурации системы и т.д.

Ключевые слова: *сетевой трафик, сценарий, элементарная компьютерная атака, комплексная компьютерная атака, воздействие на файл, инцидент информационной безопасности.*

COMPLEX COMPUTER ATTACKS GENERATING SOFTWARE TOOL USED FOR SIEM SYSTEMS SIMULATION TESTING

The article presents elementary and complex computer attacks models, information security events and incidents models, and also describes software tool for information security incident management systems (SIEM systems) simulation testing, implemented as a complex computer attacks generator. It is designed to carry out a targeted attack on the nodes of the network infrastructure controlled by the SIEM system. Complex computer attacks that created in the form of network traffic are described by a scenario, the execution of which allows us to evaluate the capabilities of SIEM to identify a wide range of information security threats - impacts on files, installation of remote administration utilities, changes in system configuration parameters, etc.

Keywords: *network traffic, scenario, simple computer attack, complex computer attack, file impact, information security incident.*

Современным вызовом для специалистов в области обеспечения информационной безопасности являются компьютерные атаки на инфраструктуру информационных систем (ИС) [1], направленные на получение несанкционированного доступа к информации (НСД) и/или отказ в обслуживании. Рост их количества и номенклатуры вынуждает владельцев ИС постоянно обновлять и совершенствовать стратегии защиты информации, повышать квалификацию персонала для противодействия компьютерным атакам и использовать новейшие программные и программно-аппаратные средства обеспечения ИБ.

Одним из решений, направленных на усиление мер по защите информации, является применение систем управления инцидентами ИБ — SIEM (Security information and event management) систем. Основной целью их построения и функционирования [2] является значительное повышение уровня ИБ в телекоммуникационной инфраструктуре ИС за счет обеспечения возможности в режиме, близком к реальному времени, манипулировать информацией о событиях в процессе функционирования отдельных узлов и сервисов инфраструктуры и осуществлять прогнозирование в управлении событиями и инцидентами ИБ.

Проверка корректности решения задач, возложенных на SIEM, невозможна без наличия информации о событиях в инфраструктуре ИС, связанных с ИБ. Согласно [3], событием ИБ является «идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности». Инцидент ИБ — это совокупность событий ИБ.

Проверить реакцию SIEM-системы на возникновение событий ИБ возможно путем проведения заранее спланированного имитационного тестирования. Такая проверка обладает следующими преимуществами:

• набор компьютерных атак, направленных на инфраструктуру ИС, известен, что позволяет достоверно оценить корректность конфигурирования SIEM-системы по результатам ее работы;

• тестирование может охватывать значительное количество сервисов инфраструктуры ИС;

• широкий спектр реализуемых действий: воздействия на файлы ИС, внедрение и эксплуатация вредоносного программного обеспечения (ВПО), атаки типа «отказ в обслужи-

вании», подмена компонентов операционной системы, эксплуатация различных уязвимостей web-приложений и т.д.

Сопоставляя определения события ИБ [3] и компьютерной атаки [4], нетрудно установить взаимосвязь между ними: компьютерная атака является причиной события ИБ. Согласно [5], инцидент ИБ можно рассматривать как совокупность событий ИБ при проведении дальнейшего анализа.

Специалисты, зачастую, выявляют несколько связанных между собой атак, которые были реализованы, например, для получения НСД к информации или влияния на узлы инфраструктуры ИС. Совокупность связанных по назначению, разделенных по времени элементарных компьютерных атак (ЭКА) будем называть комплексной компьютерной атакой (ККА).

При проведении имитационного тестирования необходимым условием возникновения инцидента ИБ, приближенного к реальному, является вариативность применяемых ККА. Для получения полного и достоверного результата следует реализовать несколько ККА, охватывающих все типы сервисов в инфраструктуре ИС. Задача генерации атак на уязвимый сервис рассматривалась в работах [6-8], тем не менее, предлагаемые авторами решения позволяют протестировать только лишь системы обнаружения атак (СОА) и телекоммуникационное оборудование (ТКО) на предмет правильности и полноты конфигурации, а также на стойкость к атакам типа «отказ в обслуживании». В рамках статьи авторы рассматривают применение имитационного тестирования по отношению к SIEM-системам, как элементам инфраструктуры ИС, обобщающим данные из нескольких источников, в том числе от СОА и ТКО, что порождает необходимость в решении задач по реализации широкого спектра ККА. В связи с этим возникает потребность в средстве автоматизации, позволяющем генерировать множество ККА, способствующих возникновению инцидентов ИБ.

Авторами предлагается программный инструментарий – генератор, предназначенный для реализации набора ККА, обеспечения вариативности в их выборе и создании.

Введем обозначения ЭКА и ККА.

Пусть неупорядоченное множество воздействий на узлы инфраструктуры ИС и информацию, обрабатывающуюся в ней, обозначается как J:

$$\mathcal{J} = \langle\langle \mathcal{H}, \mathcal{F}, \mathcal{P} \rangle, \langle \mathcal{S} \rangle\rangle, \quad (1)$$

где:

• $\mathcal{H}$ – множество элементов, описывающих воздействия на аппаратные платформы узлов: рабочие станции, ТКО, серверы.

• $\mathcal{F}$ – множество элементов, описывающих воздействие на файлы, хранящиеся на узлах.

• $\mathcal{P}$ – множество элементов, описывающих воздействие на процессы, выполняющиеся на узлах: службы, сервисы и пр.

• $\mathcal{S}$ – множество IP-адресов.

Каждый элемент I множества $\mathcal{J}$ (1) представляет собой кортеж и обозначается следующим образом:

$$I = \langle\langle H, F, P \rangle, \langle S_{src}, S_{dest} \rangle\rangle, \quad (2)$$

где:

• $H = \langle h_1, h_2, ..., h_k \rangle$, H – совокупность воздействий на аппаратную платформу конечного узла, а h_i – воздействие на определенную часть аппаратной платформы конечного узла, $H \in \mathcal{H}$.

• $F = \langle f_1, f_2, ..., f_l \rangle$, F– совокупность воздействий на файлы конечного узла, а f_i – воздействие на определенный файл, хранящийся на конечном узле, $F \in \mathcal{F}$.

• $P = \langle p_1, p_2, ..., p_m \rangle$, p – совокупность воздействий на процессы, выполняющиеся на узле, а p_i – воздействие на определенный процесс конечного узла, $P \in \mathcal{P}$.

• S_{src} – IP-адрес узла, с которого осуществляется воздействие, S_{dest} – IP-адрес конечного узла инфраструктуры $S_{src}, S_{dest} \in \mathcal{S}$.

Тогда, в соответствии с определением из [4], неупорядоченное множество ЭКА $\mathcal{A} \subset \mathcal{J}$ формируется следующим образом:

$$\forall A \in \mathcal{A}\ \exists I \in \mathcal{J}: A = I = \langle\langle H, F, P \rangle, \langle S_{src}, S_{dest} \rangle\rangle, \quad (3)$$

В соответствии с определением ЭКА из [4] выражение (3) можно интерпретировать следующим образом: целенаправленное и несанкционированное воздействие является атакой.

В целях расширения вариативности ЭКА А введем коэффициент реализации атаки $g \in \{0,1\}$, где 1 соответствует реализованной ЭКА, 0 – нереализованной.

Исходя из (2), (3) и заданного ранее определения ККА следует, что ее можно представить следующим образом:

$$C = \bigcup_{i=1}^{n} \langle g_i, A_i, \Delta t_i, T_i \rangle, \quad (4)$$

где C – ККА, A_i – ЭКА, n – количество ЭКА, составляющих ККА, g_i – коэффициент реализации атаки ЭКА, Δt_i описывает временной интервал между отправкой сетевых пакетов, а T_i – время между ЭКА.

Для проведения тестирования необходимо подготовить ЭКА, которые направлены на эксплуатацию уязвимостей в сервисах проверяемой инфраструктуры ИС. Достижение наилучших результатов возможно при использовании нескольких ККА на каждый узел инфраструктуры. Создание реалистичной ККА осуществляется в соответствии с выражением (4).

Процесс подготовки ККА заключается в формировании файлов сетевого трафика в формате pcap, которые содержат атаки, приводящие к возникновению инцидента ИБ. При создании pcap-файлов необходимо учитывать, что максимальная эффективность их последующего использования достигается в том случае, когда части каждой ЭКА записаны в отдельные файлы: подготовительные действия (перенаправление пользователя на зараженный ресурс, сканирование узла), удачные и неудачные попытки эксплуатации уязвимости и т.д.

Такой подход обеспечивает возможность применения записанных ЭКА в нескольких ККА, без необходимости повторной записи дампа сетевых пакетов.

Для проведения ККА на инфраструктуру ИС необходимо использовать сценарий — логически определенную последовательность атак А, связанных по смыслу и разделенных по времени. Сценарий является основой формируемого инцидента ИБ и создается специалистом, проводящим тестирование SIEM-системы. Одной из функциональных возможностей предлагаемого в статье генератора является воспроизведение созданных сценариев. Пример сценария представлен на рис. 1.

```
<?xml version="1.0" encoding="UTF-8"?>
<xml>
  <Scenario>
      <Title>
            Атака на рабочую станцию компании
      </Title>
      <HostDescription>
            Операционная система: Microsoft Windows 7  Professional x64
            Используемое программное обеспечение:
            - Microsoft Office 2013 Professional
            - Архиватор 7-Zip
            - Средство просмотра файлов в формате PDF Adobe Reader DC 15.006.30097
      </HostDescription>
      <ScenarioText>
            20 января 2019 года на рабочую станцию была проведена комплексная компьютерная атака (ККА),
            которая привела к возникновению инцидента информационной безопасности.
            Начало ККА зафиксировано в 16:31:12.

            Виды проведенных атак.
            - MS13-073 - удаленное выполнение кода в Microsoft Excel 2013
            - CVE-2017-16416 - удаленное выполнение кода в Adobe Reader DC 15.006.30097
            - MS17-010 - удаленное выполнение кода в SMBv1
      </ScenarioText>
      <NetworkParameters>
            <SourceIP>89.223.54.0/24</SourceIP>
            <DestinationIP>192.168.2.0/24</DestinationIP>
      </NetworkParameters>
  </Scenario>
  <Stages>
    <Date>20.01.2019 16:31:12</Date>
    <Stage id="0">
      <Min>0</Min>
      <Name>MS13-073.pcap</Name>
      <Description>Удаленное выполнение кода в Microsoft Excel 2013.</Description>
    </Stage>
    <Stage id="1">
      <Min>4</Min>
      <Name>CVE-2017-16416.pcap</Name>
      <Description>Удаленное выполнение кода в Adobe Reader DC 15.006.30097.</Description>
    </Stage>
    <Stage id="2">
      <Min>2</Min>
      <Name>MS17-010.pcap</Name>
      <Description>Удаленное выполнение кода в SMBv1.</Description>
    </Stage>
  </Stages>
</xml>
```

Рис. 1. Пример сценария

Сценарий формируется на основе файла формата XML и несет в себе следующую информацию:

• название сценария и его описание;

• описание атакуемого узла в инфраструктуре ИС;

• диапазон IP-адресов отправителя Ssrc и получателя Sdest;

• ЭКА A и интервалы T между их запусками;

• дата и время проведения ККА C.

Следует отметить, что успешность реализации атаки g определяется специалистом, разрабатывающим сценарий на этапе записи pcap-файлов сетевого трафика. Параметр Δt зависит от производительности оборудования, осуществляющего сетевое взаимодействие, и не регулируется в рамках сценария.

В сценарии, представленном на рис. 1, значение *n*, применяемое в выражении (4), равно 3. Таким образом, $C = \{\langle g_1, A_1, \Delta t_1, T_1\rangle, \langle g_2, A_2, \Delta t_2, T_2\rangle, \langle g_3, A_3, \Delta t_3, T_3\rangle\}$. Добавление интервалов *T* между запусками атак *A* призвано имитировать действия злоумышленника при осуществлении реальной атаки на ресурс ИС.

Выбор значения *g* осуществляется специалистом исходя из необходимости проверки сервисов на наличие уязвимостей во время проведения имитационного тестирования. В результате, формирование каждого pcap-файла с ЭКА для последующего применения в сценариях происходит по алгоритму, представленному на рис. 2:

Сформированный набор из pcap-файлов и сценария в формате XML добавляется в генератор. Просмотреть список всех имеющихся файлов с компьютерными атаками и выбрать необходимый для добавления к новому сценарию возможно с использованием графического web-интерфейса генератора, представленного на рис. 3.

В целях упрощения интеграции генератора в инфраструктуру ИС для проведения имитационного тестирования SIEM-систем в него добавлена функция, которая автоматически изменяет IP-адреса источника и получателя на используемые в сценариях. Указанная возможность обеспечивает вариативность параметров S_{src} и S_{dest} без участия специалиста, проводящего тестирование.

Процесс изменения адресов запускается после добавления новых pcap-файлов с ЭКА к сценарию и изменения информации в полях «Диапазон адресов источника» и «Диапазон адресов назначения» на странице сценария. В результате любой трафик, содержащий ЭКА, подстраивается под адресное пространство сети инфраструктуры ИС.

Применение представленного генератора при проведении имитационного тестирования происходит в соответствии со следующим алгоритмом:

1. выбор необходимого сценария. В случае, если сценарий отсутствует, его следует создать;

2. запуск сценария;

3. обработка специалистом результатов работы SIEM-системы;

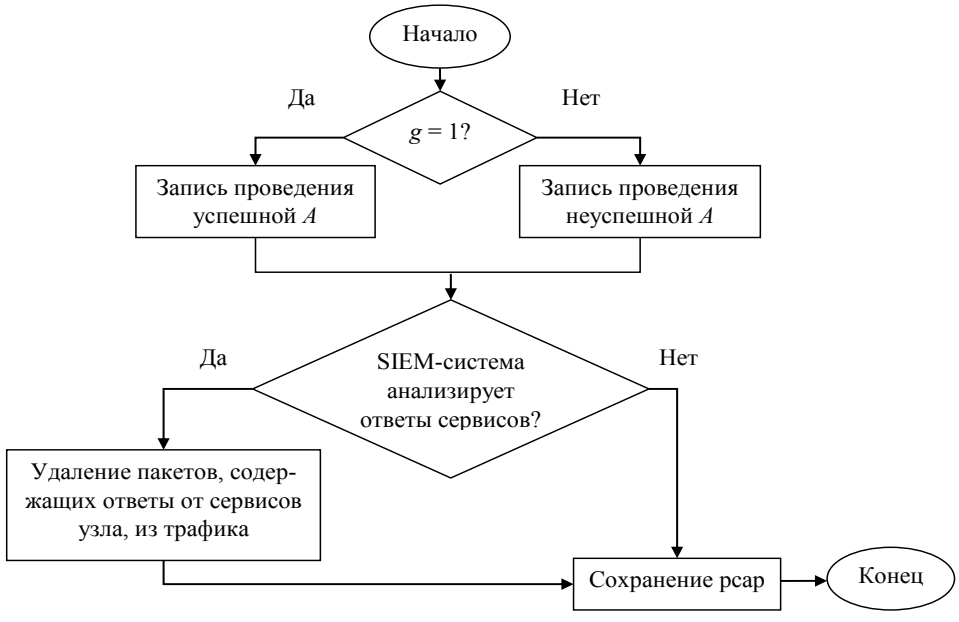

Рис. 2. Алгоритм формирования pcap-файла сетевой компьютерной атаки

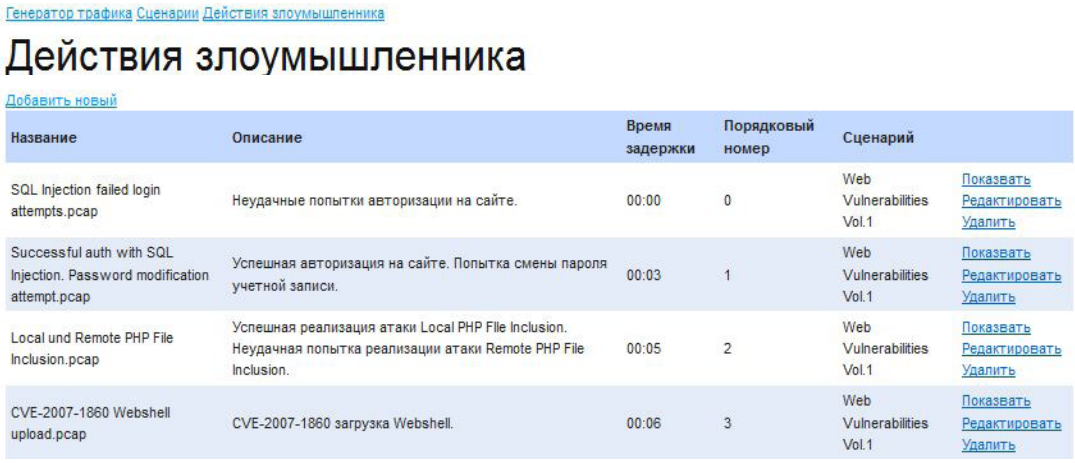

Рис. 3. Web-интерфейс генератора

4. формирование предложений по совершенствованию конфигурации SIEM-системы.

Генерация потока пакетов с ЭКА приводит к возникновению событий ИБ вследствие того, что проводимые атаки будут зафиксированы SIEM-системой.

Зададим обозначения события и инцидента ИБ.

Пусть неупорядоченное множество событий ИБ обозначается как $\mathcal{E}$:

$$\mathcal{E} = \langle H^*, F^*, P^* \rangle, \quad (5)$$

где:

• $\mathcal{H}^*$ – множество элементов, описывающих состояния аппаратных платформ узлов инфраструктуры ИС.

• $\mathcal{F}^*$ – множество элементов, описывающих состояния файлов, хранящихся на узлах.

• $\mathcal{P}^*$– множество элементов, описывающих состояние процессов, выполняющихся на узлах: службы, сервисы и пр.

Каждый элемент E множества $\mathcal{E}$ (5) представляет собой кортеж и обозначается следующим образом:

$$E = \langle H^*, F^*, P^* \rangle, \quad (6)$$

где:

• $H^* = \langle h_1^*, h_2^*, ..., h_k^* \rangle$, H^* – совокупность состояний аппаратной платформы конечного узла, а h_i^*– состояние определенной части аппаратной платформы конечного узла, $H^* \in \mathcal{H}^*$.

• $F^* = \langle f_1^*, f_2^*, ..., f_l^* \rangle$, F^* – совокупность состояний файлов конечного узла, а f_i^* – состояние определенного файла, хранящегося на конечном узле, $F^* \in \mathcal{F}^*$.

• $P^* = \langle p_1^*, p_2^*, ..., p_m^* \rangle$, P^* – совокупность состояний процессов, выполняющихся на узле, а p_i^*– состояние определенного процесса конечного узла, $P^* \in \mathcal{P}^*$.

Стоит отметить, что $\mathcal{H}$ и $\mathcal{H}^*$, $\mathcal{F}$ и $\mathcal{F}^*$, $\mathcal{P}$ и $\mathcal{P}^*$ не связаны между собой отображениями: множества расположены над различными полями – воздействий и состояний соответственно.

Исходя из (6) и заданного ранее определения инцидента ИБ, справедливо соотношение:

$$R = \bigcup_{j=1}^{n'} \langle m_j, E_j \rangle$$

где R – инцидент ИБ, E_j – событие ИБ, n' – количество событий ИБ, потенциально обнаруживаемых SIEM-системой, а m_j– коэффициент соответствия, причем $m_j \in \{-1, 0, 1\}$, где 1 соответствует корректно определенному E_j, 0 – его отсутствию, –1 соответствует наличию неверно идентифицированного E_j. В общем случае следует учитывать, что n' не всегда равен n, так как Ej может быть результатом проведения нескольких A. Коэффициент m_j позволяет специалисту оценить корректность правил функционирования SIEM-системы.

Анализ журналов сообщений, полученных в рамках 2 и 3 шагов алгоритма, согласно [5], является основополагающей информацией, получаемой в ходе расследования инцидента ИБ R.

Наличие известного сценария и обнаруженных недостатков в применяемых мерах обеспечения ИБ позволяют существенно упростить процесс формирования рекомендаций по усовершенствованию настроек SIEM-системы (шаг 4 алгоритма применения генератора ККА). Стоит отметить, что предложенный алгоритм не вносит расхождений с методами и средствами, используемыми в [5], а лишь дополняет их.

К преимуществам предложенного инструментария стоит отнести возможность автоматизации действий потенциального злоумышленника для определения недостатков применяемой SIEM-системы.

Созданный генератор применяется в составе компьютерного полигона «ГосСОПКА» учебно-научного центра «Информационная безопасность» Института радиоэлектроники и информационных технологий-РТФ Уральского федерального университета имени первого Президента России Б.Н. Ельцина. Используется при проведении лабораторных работ и практических занятий для студентов, проходящих обучение по направлению 10.03.01 «Информационная безопасность» и специальностям 10.05.01 «Компьютерная безопасность», 10.05.02 «Информационная безопасность телекоммуникационных систем».

Литература

1. ISO/IEC 2382:2015. Information technology — Vocabulary [Электронный ресурс]. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en (дата обращения: 30.07.2019)

2. Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. Вып.1 (20). СПб.: Наука, 2012. — С. 27–56.

3. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. (ISO/IEC TR 18044:2004 «Information technology — Security techniques — Information security incident management»). — М. : ФГУП «Стандартинформ», 2007. — 50 с.

4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения [Электронный ресурс]. URL: https://docs.cntd.ru/document/gost-r-51275-2006 (дата обращения: 30.07.2019)

5. СТО БР ИББС-1.3-2016. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств [Электронный ресурс]. URL: https://www.cbr.ru/Content/Document/File/46920/st-13-16.pdf (дата обращения: 30.07.2019)

6. Хорьков Д.А. Методы тестирования сетевых систем обнаружения компьютерных атак // Научно-техническая информация. Серия 1. Организация и методика информационной работы. № 6. — М.: ВИНИТИ РАН, 2012. — С. 9–15.

7. Хорьков Д.А., Гайдамакин Н.А. Модель атакующего воздействия на автоматизированные системы в рамках развития аппарата сетей Петри // Проблемы информационной безопасности. Компьютерные системы. № 1. СПб: Санкт-Петербургский государственный политехнический университет, 2013. — С. 73–80.

8. Агафонов А.В. Структура и принципы работы комплекса тестирования устойчивости телекоммуникационного оборудования к сетевым атакам типа «отказ в обслуживании» [Текст] / А.В. Агафонов, Н.И. Синадский // Вестник УрФО. Безопасность в информационной сфере. — Челябинск : Издательский центр ЮУрГУ, 2015. — Вып. 18. — С. 4–11.

References

1. ISO/IEC 2382:2015. Information technology — Vocabulary [Jelektronnyj resurs]. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en (data obrashhenija: 30.07.2019)

2. Kotenko I.V., Saenko I.B., Polubelova O.V., Chechulin A.A. Primenenie tehnologii upravlenija informaciej i sobytijami bezopasnosti dlja zashhity informacii v kriticheski vazhnyh infrastrukturah // Trudy SPIIRAN. Vyp.1 (20). SPb.: Nauka, 2012. — S. 27–56.

3. GOST R ISO/MJeK TO 18044-2007. Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Menedzhment incidentov informacionnoj bezopasnosti. (ISO/IEC TR 18044:2004 «Information technology — Security techniques — Information security incident management»). — M. : FGUP «Standartinform», 2007. — 50 s.

4. GOST R 51275-2006. Zashhita informacii. Ob#ekt informatizacii. Faktory, vozdejstvujushhie na informaciju. Obshhie polozhenija [Jelektronnyj resurs]. URL: https://docs.cntd.ru/document/gost-r-51275-2006 (data obrashhenija: 30.07.2019)

5. STO BR IBBS-1.3-2016. Obespechenie informacionnoj bezopasnosti organizacij bankovskoj sistemy Rossijskoj Federacii. Sbor i analiz tehnicheskih dannyh pri reagirovanii na incidenty informacionnoj bezopasnosti pri osushhestvlenii perevodov denezhnyh sredstv [Jelektronnyj resurs]. URL: https://www.cbr.ru/Content/ Document/File/46920/st-13-16.pdf (data obrashhenija: 30.07.2019)

6. Hor'kov D.A. Metody testirovanija setevyh sistem obnaruzhenija komp'juternyh atak // Nauchno-tehnicheskaja informacija. Serija 1. Organizacija i metodika informacionnoj raboty. № 6. — M.: VINITI RAN, 2012. — S. 9–15.

7. Hor'kov D.A., Gajdamakin N.A. Model' atakujushhego vozdejstvija na avtomatizirovannye sistemy v ramkah razvitija apparata setej Petri // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. № 1. SPb: Sankt-Peterburgskij gosudarstvennyj politehnicheskij universitet, 2013. — S. 73–80.

8. Agafonov A.V. Struktura i principy raboty kompleksa testirovanija ustojchivosti telekommunikacionnogo oborudovanija k setevym atakam tipa «otkaz v obsluzhivanii» [Tekst] / A.V. Agafonov, N.I. Sinadskij // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. — Cheljabinsk : Izdatel'skij centr JuUrGU, 2015. — Vyp. 18. — S. 4–11.

ГИБИЛИНДА Роман Владимирович, ассистент учебно-научного центра «Информационная безопасность» Института радиоэлектроники и информационных технологий - Уральского Федерального Университета им. первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: gibilinda91@gmail.com.

ФАРТУШНЫЙ Андрей Владимирович, ассистент учебно-научного центра «Информационная безопасность» Института радиоэлектроники и информационных технологий - Уральского Федерального Университета им. первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: a.v.fartushnyi@urfu.ru.

GIBILINDA Roman Vladimirovich, assistant of Educational and Scientific Center "Information Security", Institute of Radio electronics and Information Technologies, Ural Federal University named after first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, Mira str., 19. E-mail: gibilinda91@gmail.com.

FARTUSHNYI Andrey Vladimirovich, assistant of Educational and Scientific Center "Information Security", Institute of Radio electronics and Information Technologies, Ural Federal University named after first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, Mira str., 19. E-mail: a.v.fartushnyi@urfu.ru.