УДК 004.089

А.И. Трубей

АНАЛИЗ ОСОБЕННОСТЕЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГРИД-СИСТЕМ

Предлагается краткий обзор особенностей обеспечения информационной безопасности грид-систем, рассматривается методика оценки рисков, угроз и уязвимостей с использованием общедоступных баз данных, экспертных систем и статистических методов.

Введение

В настоящее время развитие вычислительных технологий достигло своего пика, когда простое увеличение мощности процессоров, объема хранилищ данных, пропускной способности сети передач практически исчерпало свои ресурсы и не удовлетворяет растущим потребностям к вычислительным ресурсам как в науке, образовании, так и в решении сложных прикладных задач. Скорость сетевого взаимодействия становится все более сопоставимой со скоростью процессоров, и, соответственно, вопрос о локализации вычислительных мощностей постепенно теряет свою остроту. В связи с этим наблюдается тенденция сдвига в сторону распределенных вычислительных систем, которые обеспечивают доступ пользователей к географически распределенным вычислительным ресурсам, объединенным в единый мощный пул ресурсов.

Распределенные вычислительные системы уже давно применяются для решения ресурсоемких задач, но в последние годы стали изменяться масштаб и сам характер их использования. Дальнейшее развитие в этой области в будущем может позволить крупным промышленным предприятиям, научно-исследовательским организациям, а также рядовым пользователям получать доступ к гибкой, географически распределенной и масштабируемой инфраструктуре для обработки и хранения данных. Существует большое количество разнообразных видов и классификаций распределенных систем, таких как кластерные системы, грид-системы, облачные системы, пиринговые сети (peer-to-peer, P2P) и т. д.

Очевидно, что при разработке подобных сложных систем одной из важнейших задач является реализация механизмов обеспечения безопасности, связанных с необходимостью противодействия компьютерным атакам на вычислительные и информационные ресурсы грид-систем. Особые свойства грид-систем (гетерогенность, перераспределение ресурсов, высокая динамика состояний, децентрализованность управления и т. д.) создают благоприятные условия для осуществления на них таких негативных воздействий, как атаки отказа в обслуживании, распространение вредоносного программного обеспечения, несанкционированный доступ к ресурсам.

В статье детализированы меры, которые необходимо принимать для обеспечения безопасного управления в грид-системе, предложена методика оценки рисков, угроз и уязвимостей с использованием базы общеизвестных уязвимостей, имеющих строгую характеристику по описательным критериям (common vulnerabilities and exposures, CVE) и банка данных Федеральной службы по техническому и экспортному контролю России (ФСТЭК России). Кроме того, приведен метод оценки инцидентов информационной безопасности (ИБ) на основе использования критерия χ^2.

1. Обеспечение безопасного управления в грид-системе

Безопасное управление требует контроля доступа к услугам через надежные протоколы безопасности и в соответствии с принятой политикой безопасности. Например, получение прикладных программ и запуск их в грид-среде может потребовать аутентификации и идентификации. Совместное использование ресурсов пользователями требует наличия какого-нибудь вида механизма изоляции. Кроме того, необходимы стандартные механизмы безопасности, которые могут быть направлены на защиту грид-систем путем поддержки безопасного совместного использования ресурсов между административными доменами [1].

Эффективность принимаемых мер защиты информации зависит от качества определения угроз безопасности информации конкретной грид-системы в конкретных условиях ее функционирования. Они, как правило, включают следующие меры защиты:

1. Аутентификацию и идентификацию. Для идентификации индивидуальных пользователей и установления запрашиваемых сервисов необходимы соответствующие механизмы аутентификации. Грид-система должна удовлетворять требованиям политики безопасности каждого домена, а также, возможно, определять пользовательские политики безопасности. Аутентификация и идентификация должны включать различные модели контроля доступа и их реализации [1]. Особенностями аутентификации и идентификации в грид-системе являются единый вход и делегирование прав.

Единый вход. Пользователь должен аутентифицироваться только один раз в начале сеанса работы, получая доступ ко всем разрешенным ресурсам базового уровня архитектуры грид-системы. Технология единого входа позволяет избежать повторной процедуры аутентификации во вторичных доменах. Применение данного подхода:

– сокращает время, затрачиваемое пользователем на аутентификацию в каждом домене;

– повышает безопасность за счет сокращения аутентификационной информации, которую необходимо запоминать пользователю;

– сокращает время, затрачиваемое системным администратором на управление учетными записями;

– сокращает нагрузку на серверы доступа за счет уменьшения количества процедур аутентификации.

Делегирование прав (доверия к аутентификатору). Важным условием для эффективной работы распределенных систем является возможность делегирования прав пользователя грид-сервисам. Практически любой запрос пользователя проходит через несколько сервисов. При отсутствии механизма делегирования пользователю было бы необходимо аутентифицироваться на каждом сервисе в цепочке сервисов, обрабатывающих данный запрос, т. е. пользователь после отправления задания должен постоянно отвечать на запросы о своей аутентификации от каждого сервиса в обрабатывающей цепочке. Это усложняет работу в грид-системе – во всяком случае при запуске большого набора заданий. Делегирование прав позволяет этого избежать. Пользователь должен иметь возможность запуска программ от своего имени. Программы получают доступ ко всем ресурсам, к которым имеет доступ пользователь, могут делегировать часть своих прав другим программам. Риск злоупотребления делегированными правами должен быть сведен к минимуму, например, путем ограничения прав, переданных посредством делегирования на запланированную работу, и ограничения длительности их существования.

В настоящее время существует инфраструктура безопасности грид-систем (grid security infrastructure, GSI), которая обеспечивает безопасную работу в незащищенных сетях общего доступа, предоставляя такие сервисы, как аутентификация, конфиденциальность передачи информации и единый вход в грид-систему. Поскольку вычислительной платформой для решения пользовательских задач в грид-системе являются связанные компьютеры, а не серверы (как это реализовано в кластерных системах и системах облачных вычислений), важной задачей обеспечения защиты данных пользователей грид-систем от атак несанкционированного доступа является изоляция указанных данных от воздействия факторов хостовой среды [2]. Инфраструктура GSI основана на надежных и широко используемых сервисах инфраструктуры криптографии с открытым ключом (public key infrastructure, PKI), которые наиболее подробно описаны в рекомендациях ITU-T X.842 [3].

Основными механизмами аутентификация в PKI являются:

– установление доверия на базе определенной модели доверия;

– система именования субъектов, обеспечивающая уникальность имени в рамках данной системы;

– связь имени субъекта и пары ключей (открытый и закрытый) с подтверждением этой связи средствами удостоверяющего центра (УЦ), которому доверяет субъект, проверяющий правильность связи.

Для обеспечения высоких уровней доверия к результатам аутентификации при доступе сотрудников государственных организаций к информационным системам (в том числе и к грид-ресурсам) все чаще используются так называемые смарт-карты с неизвлекаемым секретным ключом [4]. Они способны безопасно генерировать внутри чипа ключевой материал. Устройства генерируют две ключевые пары. Первая пара используется для организации доступа к сети и информационным ресурсам. На открытый ключ первой пары УЦ выпускается сертификат, который применяется для управления доступом. Вторая пара ключей используется для электронно-цифровой подписи (ЭЦП): открытый ключ пересылается в УЦ для формирования сертификата ключа проверки подписи на основе тщательной идентификации владельца, все этапы которой протоколируются.

Неизвлекаемость закрытых ключей гарантируется требованиями к чипам смарт-карт, закрепленными Федеральными стандартами обработки информации (federal information processing standards, FIPS), в частности стандартом FIPS-140 и уровнем доверия не ниже EAL4+ (уровнем гарантии оценки УГО4+ в гармонизированном стандарте СТБ 34.101.3–2014 [5]). Аутентификатор представляет собой аппаратный криптографический модуль, прошедший проверку соответствия FIPS-140-2 уровня 2 и выше. Для аутентификации требуется, чтобы заявитель по безопасному протоколу аутентификации подтвердил принадлежность данного аутентификатора именно ему, а также возможность управления аутентификатором.

Неизвлекаемость секретного ключа означает то, что он не покидает чипа, внутри которого его сгенерировали в составе ключевой пары. Все внешние функции (запрос на сертификат, проверку подписи и т. д.) выполняет открытый ключ. Частным случаем применения таких устройств является решение одной из самых сложных задач – проблемы неотказуемости от подписи с помощью ЭЦП документа или сообщения.

Наиболее популярным способом аутентификации пользователей является аутентификация по паролю. Одним из направлений усовершенствования этого способа может стать применение усиленной аутентификации путем добавления дополнительных признаков, в том числе ритма набора пароля, например, по ритму определенной мелодии. На первоначальном этапе пользователь вводит пароль с заданным ритмом, интервалы между нажатиями клавиш сохраняются в памяти компьютера как эталонный образец и при последующих входах этот образец сравнивается с новыми наборами пароля [6].

Многофакторная, или расширенная, аутентификация основана на совместном использовании нескольких факторов аутентификации (знаний, средств или объектов хранения одной из информационных составляющих легитимной процедуры аутентификации), что значительно повышает безопасность использования информации по меньшей мере со стороны пользователей, подключающихся к информационным системам по защищенным и незащищенным каналам коммуникаций. В настоящее время самым популярным вторым фактором, используемым поставщиками сервиса, является одноразовый пароль (one time password, OTP). Кроме того, в качестве дополнительной опции для определения прав доступа к информационным ресурсам используются биометрические данные человека (отпечатки пальцев, изображение лица и т. д.). Главное преимущество биометрической идентификации заключается в том, что идентифицируется конкретный человек, а не отчужденный носитель (карта, жетон и т. д.) или пароль. Биометрический идентификатор нельзя забыть, украсть или передать [7].

2. Обмен политиками безопасности. Потребители и поставщики сервисов должны иметь возможность динамически обмениваться информацией о политиках безопасности, чтобы установить путем переговоров контекст безопасности между ними [1]. Обмен политиками безопасности – предоставление возможности обмена информацией о политиках безопасности вызывающей и вызываемой сторонам для создания безопасной среды обмена информацией. Каждый ресурс может использовать любой из существующих способов решения проблемы безопасности системы. Реализация системы безопасности грид-систем должна взаимодействовать с этими локальными системами безопасности, не изменяя их. Пользователи должны иметь возможность создавать новые сервисы (ресурсы) динамически, без вмешательства администратора. Эти сервисы должны координироваться и безопасно взаимодействовать с другими сервисами. Доступ к ним должен предоставляться без противоречий с локальной политикой безопасности.

2. Предотвращение вторжений, оценка рисков, угроз и уязвимостей с использованием общедоступных баз данных

В соответствии с приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 16.01.2015 № 3 [8] «в целях реализации политики информационной безопасности разрабатываются локальные нормативные правовые акты организации, регламентирующие порядок:

– защиты от вредоносного программного обеспечения;

– выявления угроз, которые могут привести к сбоям, нарушению функционирования информационной системы;

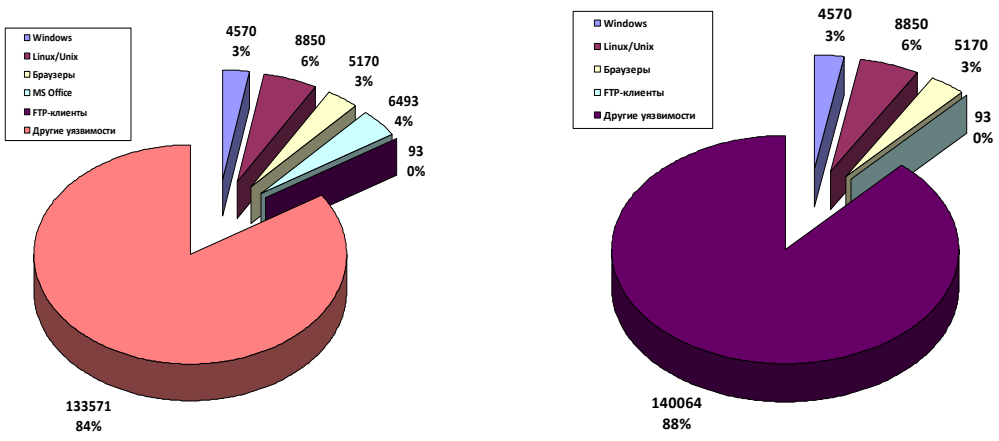
– реагирования на инциденты информационной безопасности…».

Угрозы безопасности информации в грид-системе определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации. В грид-системе должно обеспечиваться обнаружение (предотвращение) угроз, вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к информации, специальных воздействий на информацию (носители информации) в целях ее хищения, уничтожения, искажения и блокирования доступа к ней [9]. Для обнаружения и идентификации злоупотреблений (в том числе действий вирусов) необходима мощная система мониторинга. Для защиты критически важных областей или функций необходимо обеспечить возможность перемещения этих областей для отвода от них атаки [1].

Адекватным ответом на разветвленный и многоуровневый характер процессов реализации угроз в грид-системах, огромное количество пользователей, изменчивость их состава и предоставляемых им услуг является создание так называемых многоагентных систем защиты. В настоящее время создаются системы защиты с централизованным принципом построения, а в многоагентных системах в основном применяется централизованно-децентрализованный принцип построения.

При централизованном принципе все элементы системы защиты замыкаются на консоль администратора безопасности. В многоагентных системах так называемые агенты (программные или программно-аппаратные компоненты) реализуют предопределенные функции безопасности. Они взаимодействуют между собой, обмениваются сообщениями на языке высокого уровня для принятия согласованных решений, адаптируются к реконфигурации сети, изменению трафика и новым видам атак и иным нарушениям безопасности информации, используют алгоритмы обучения, инициализируют деятельность других агентов и решают, таким образом, весь необходимый комплекс задач защиты информации в информационной системе [10].

Для идентификации и анализа уязвимостей и угроз, как правило, используется база общеизвестных уязвимостей CVE [10, 11] (рисунок).



а) *б)*

Структура уязвимостей согласно базе CVE: *а)* в грид-системах; *б)* в суперкомпьютерных системах

Кроме того, для анализа уязвимостей и угроз, наиболее характерных для государственных информационных систем, может также использоваться банк данных угроз безопасности информации ФСТЭК России [12]. В настоящее время в списке угроз банка содержатся 182 идентифицированные угрозы для различных типов развертывания информационных систем. В частности, согласно данному списку для грид-систем актуальными являются угрозы:

УБИ.001 – автоматического распространения вредоносного кода в грид-системе;

УБИ.002 – агрегирования данных, передаваемых в грид-системе;

УБИ.047 – нарушения работоспособности грид-системы при нетипичной сетевой нагрузке;

УБИ.081 – несанкционированного доступа к локальному компьютеру через клиента грид-системы;

УБИ.110 – перегрузки грид-системы вычислительными заданиями;

УБИ.147 – распространения несанкционированно повышенных прав на всю грид-систему.

Для суперкомпьютерных систем актуальными будут угрозы:

УБИ.029 – использования вычислительных ресурсов суперкомпьютера «паразитными» процессами;

УБИ.106 – отказа в обслуживании системой хранения данных суперкомпьютера;

УБИ.146 – прямого обращения к памяти вычислительного поля суперкомпьютера;

УБИ.161 – чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями.

В базу данных уязвимостей банка включено около 13 000 идентифицированных уязвимостей, в том числе значительное количество уязвимостей, характерных только для грид-систем. В частности, УБИ 001 может быть реализована при условии наличия у нарушителя привилегий легального пользователя грид-системы, например, с использованием уязвимости 2014-00013 (табл. 1).

Таблица 1

Описание и основные параметры уязвимости 2014-00013

Параметр	Содержание
Описание уязвимости	Система обмена программными сообщениями Apache Qpid содержит уязвимость, связанную с ошибкой в механизме аутентификации во время обработки теневых подключений AMQP-клиентов. С помощью специально сформированного запроса злоумышленник может представиться законным пользователем
Вендор	Apache Software Foundation
Наименование ПО	Apache Qpid
Версия ПО	0.16, 0.14
Тип ПО	Сетевое ПО
Операционные системы и аппаратные платформы	Сообщество свободного программного обеспечения Linux.x64; сообщество свободного программного обеспечения Linux.x86; Microsoft Corp. Windows.x64; Microsoft Corp. Windows.x86
Тип ошибки	Неправильная аутентификация
Класс уязвимости	Уязвимость архитектуры
Дата выявления	22.06.2012
Базовый вектор уязвимости	AV:N/AC:L/Au:N/C:N/I:P/A:N
Уровень опасности уязвимости	Средний уровень опасности (базовая оценка CVSS составляет 5)
Возможные меры по устранению уязвимости	Обновление ПО до версии 0.17 или выше
Статус уязвимости	Подтверждена производителем
Наличие эксплойта	Существует
Информация об устранении	Уязвимость устранена
Идентификаторы других систем описаний уязвимостей	CVE: CVE-2012-3467 OSVDB: OSVDB ID:84562
Язык разработки ПО	Java, C++

Для примера оценим риск реализации угрозы автоматического распространения вредоносного кода в грид-системе (УБИ 001) посредством эксплуатации уязвимости 2014-00013 с использованием наиболее распространенной, востребованной и проверенной на практике системы оценки общеизвестных уязвимостей (common vulnerability scoring system, CVSS 2.0) [13–15], которая состоит из трех групп метрик (критериев).

Величина риска, соответствующая прогнозируемым среднегодовым потерям в результате инцидентов безопасности ALE (annual loss expectancy), определяется по формуле [15]

$$ALE = AV^* \cdot EF \cdot ARO, \quad (1)$$

где AV^* (asset value) – стоимость подвергаемых риску активов грид-системы (данных, программ, аппаратуры и т. д.);

EF (exposure factor) – степень уязвимости актива к угрозе;

ARO (annualized rate of occurrence) – среднегодовая частота возникновения инцидентов (величина, представляющая собой ожидаемую частоту реализации угрозы в год).

На основании анализа основных параметров уязвимости 2014-00013 и конкретной среды эксплуатации грид-системы определим значения базовых, временных и контекстных метрик данной уязвимости, которые приведены в табл. 2 (выделены соответствующими цветами).

Таблица 2

Значения метрик уязвимости 2014-00013

Базовые метрики (BM)			Временные метрики (TM)					Контекстные метрики (EM)					
Вектор доступа (AV)			Возможность использования (E)					Возможность косвенного ущерба (CDP)					
L	A	N	ND	U	POC	F	H	ND	N	L	LM	MN	H
Сложность доступа (AC)			Уровень исправления (RL)					Плотность целей (TD)					
H	M	L	ND	OF	T	W	U	ND	N	L	M	H	
Аутентификация (AU)			Степень достоверности источника (RC)					Требования к конфид. (CR)					
M	S	N	ND	UC	UR	C		ND	L	M	H		
Влияние на конфид. (C)								Требования к целостности (IR)					
N	P	C						ND	L	M	H		
Влияние на целостность (I)								Требования к доступности (AR)					
N	P	C						ND	L	M	H		
Влияние на доступность (A)													
N	P	C											

Базовые метрики (BM). Значения базовых метрик определены в базовом векторе уязвимости (AV:N/AC:L/Au:N/C:N/I:P/A:N) (см. табл. 1).

Временные метрики (TM). С помощью метрики «возможность использования» (E) измеряется существующее состояние доступности кода или метода эксплуатации уязвимости. В табл. 1 указано, что эксплойт существует, поэтому согласно [14] E примет значение F (функциональная). Это означает, что функциональный код эксплойта доступен и применим в большинстве ситуаций, где существует уязвимость. Метрика «уровень исправления» (RL) примет

значение OF (официальное исправление), так как в табл. 1 официально информируется, что уязвимость устранена. Метрика «степень достоверности источника» (RC) примет значение C (подтверждено), так как в табл. 1 сообщается, что статус уязвимости подтвержден производителем.

Контекстные метрики (EM). Являются необязательными и отражают характеристики уязвимости, которые относятся к конкретной среде эксплуатации и характерны только для нее. Контекстные метрики определяются пользователями, поскольку они точнее могут оценить потенциальное воздействие уязвимости в рамках своей собственной среды. У нас нет полных сведений о конкретной используемой или проектируемой грид-системе, поэтому значения данных метрик будем задавать ориентировочно (на основании опыта, здравого смысла и общих сведений об аналогичных системах).

Метрике «возможность косвенного ущерба» (CDP) присвоим значение LM (от низкой до средней). Это означает, что может иметь место умеренная потеря дохода или производительности грид-системы. Метрике «плотность целей» (TD) присвоим значение L (низкое), т. е. риску подвержено от 1 до 25 % всех систем среды. Метрикам «требования к конфиденциальности» (CR) и «требования к доступности» (AR) присвоим значение ND (не определено), так как базовые метрики «влияние на конфиденциальность» (C) и «влияние на доступность» (A) принимают значение N (отсутствует). Метрике «требования к целостности» (IR) присвоим значение M (среднее), так как базовая метрика «влияние на целостность» (I) принимает значение P (частичное).

В результате получим суммарный вектор уязвимости:

AV:N/AC:L/Au:N/C:N/I:P/A:N/E:F/RL:OF/RC:C/CDP:LM/TD:L/CR:ND/IR:M/AR:ND.

Далее воспользуемся калькулятором CVSS [12] и получим контекстную оценку уязвимости environmental score (ES) = 1,5. Согласно шкале FortiGuard [16] уровень опасности данной уязвимости низкий. После нормирования получим [15]

$$EF = CVSS\ Rating / 10 = 0{,}15. \tag{2}$$

Определяем среднегодовую частоту возникновения инцидентов:

$$ARO = P_E \cdot F_E, \tag{3}$$

где P_E – вероятность использования уязвимости;

F_E – количество попыток в год, когда имелась принципиальная возможность осуществить эксплуатацию уязвимости.

Вероятность эксплуатации уязвимости вычисляется по формуле [15]

$$P_E = AV \cdot AC \cdot Au \cdot E \cdot RL \cdot RC = 1 \cdot 0{,}71 \cdot 0{,}704\ 0{,}95 \cdot 0{,}87 \cdot 1 = 0{,}4. \tag{4}$$

Стоимость подвергаемых риску активов AV^* и прогнозируемых частот реализации конкретных угроз (инцидентов ИБ) F_E определяется с использованием аппарата теории вероятностей и математической статистики, аналитических методов, а также экспертных оценок. В разд. 3 предложен один из таких статистических методов, основанный на теоретических и экспериментальных исследованиях.

Приведем конкретный пример расчета величины риска. Предположим, что прибыль от работы некоторой условной коммерческой грид-системы составляет 750 млн руб. в месяц. В результате автоматического распространения вредоносного кода грид-система (или один из ее узлов) вышла из строя. На восстановление ее работоспособности планируется затратить одни сутки. Стоимость затрат на ремонт составит примерно 25 млн руб. По формуле (2) определяем степень уязвимости грид-системы к угрозе реализации нелегитимных действий нарушителем EF = 0,15. Вероятность осуществления нарушителем нелегитимных действий (например, по уровню квалификации) вычисляем по формуле (4) – P_E = 0,4. Количество попыток в год, когда нарушитель в принципе может осуществлять такие действия (например, посещает

объекты грид-системы), определяем из опыта или статистических данных – F_E = 10. Далее вычисляем AV^* = 750/30 + 25 = 50. По формуле (3) определяем ARO = 0,4·10 = 4. Следовательно, в соответствии с формулой (1)

$$ALE = AV^* \cdot EF \cdot ARO = 50 \cdot 0{,}15 \cdot 4 = 30 \text{ млн руб.}$$

Аналогичным образом можно оценить риски реализации других угроз.

3. Статистические методы оценки информационных атак

Для анализа угроз на основе накопленных данных об инцидентах ИБ могут применяться различные статистические методы. Предлагается метод оценки инцидентов, которые связаны с реализацией возможных угроз, воздействующих на систему, на основе использования критерия χ^2 [17].

Предположим, что частоты инцидентов, связанных с реализацией угроз $E_1, E_2, ..., E_i, ..., E_r$ за промежуток времени T_1 (например, за текущий месяц, квартал, год), составляют $\mu_1, \mu_2, ..., \mu_i, ..., \mu_r$; частоты инцидентов, связанных с реализацией тех же угроз $E_1, E_2, ..., E_i, ..., E_r$ за промежуток времени T_2 (например, за прошлый месяц, квартал, год), – соответственно $\nu_1, \nu_2, ..., \nu_i, ..., \nu_r$.

Используем критерий χ^2 для сравнения данных последовательностей частот на предмет их однородности. Выясним, не произошли ли изменения в распределении вероятностей реализации угроз во временном промежутке T_2 по сравнению с временным промежутком T_1. Для этого вычислим статистику [17]:

$$\chi^2 = m \cdot n \sum_{i=1}^{r} \frac{1}{\mu_i + \nu_i} \left(\frac{\mu_i}{m} - \frac{\nu_i}{n} \right)^2, \tag{5}$$

где $m = \sum_{i=1}^{r} \mu_i$, $n = \sum_{i=1}^{r} \nu_i$.

Данная статистика при больших объемах выборок m и n имеет распределение χ^2 с $r-1$ степенями свободы. Проверяемая гипотеза об однородности отклоняется, когда вычисленное значение статистики χ^2 больше критического значения χ^2_α, или достигнутый уровень значимости (p-value) [17]

$$p = p(\chi^2 > \chi^2_p) = \frac{1}{2^{\frac{r-1}{2}} \Gamma\left(\frac{r-1}{2} \right)} \int_{\chi^2_p}^{\infty} x^{\frac{r-1}{2}-1} e^{-\frac{x}{2}} dx \tag{6}$$

меньше заданного уровня значимости (заданной вероятности ошибки первого рода) α, где $\Gamma\left(\frac{r-1}{2} \right)$ – гамма-функция Эйлера.

Проиллюстрируем применение предложенного метода на примере отчетов JSOC Security flash report, которые основаны на данных, полученных в коммерческом центре мониторинга и реагирования на инциденты ИБ JSOC (jet security operation center) [18]. Отчеты являются сводными материалами и результатами анализа инцидентов, выявленных командой JSOC как в рамках оказания регулярных услуг мониторинга и реагирования на инциденты, так и в качестве консультативно-аналитической поддержки компаний российского рынка. Они предназначены для информирования служб информационных технологий и ИБ об основных трендах, касающихся угроз ИБ.

Рассмотрим внутренние инциденты, т. е. инциденты, инициаторами и причиной которых становились действия внутренних сотрудников клиентов JSOC: халатность в соблюдении политик ИБ или их прямое нарушение, компрометация или передача учетных данных сотрудников, злонамеренные и незлонамеренные воздействия на бизнес-процессы и функционирование

систем клиентов. К внутренним пользователям – инициаторам инцидента – относятся все пользователи с возможностью доступа в локальную сеть без преодоления периметра, в том числе подрядчики и контрагенты. Сводные частоты данных инцидентов приведены в табл. 3.

Таблица 3

Статистика по внутренним инцидентам за третий и второй кварталы 2014 г.

Суммарные частоты инцидентов		Частоты инцидентов, связанных с реализацией типов угроз						
		E_1	E_2	E_3	E_4	E_5	E_6	E_7
		Утечка конфиденциальных данных	Нарушение политик доступа в Интернет	Несанкционированные активности в рамках удаленного доступа	Компрометация внутренних учетных записей	Нелегитимные изменения в ИТ-системах	Вирусные атаки, включая ransomware, zero-day	Нелегитимная работа с привилегир. учетными записями и прочие инциденты
3 кв.	m	μ_1	μ_2	μ_3	μ_4	μ_5	μ_6	μ_7
	11 692	3 028	2 011	573	1 649	935	1 380	2 116
2 кв.	n	ν_1	ν_2	ν_3	ν_4	ν_5	ν_6	ν_7
	10 891	2 962	1 775	468	1 579	915	1 232	1960

С помощью статистики χ^2 оценим, произошли ли изменения в распределении частот внутренних инцидентов в третьем квартале по сравнению со вторым кварталом. По формуле (5) получим значение $\chi^2 = 13{,}72$ (для шести степеней свободы), которое не превышает критического значения $\chi^2_{6,p} = 16{,}81$, соответствующего согласно формуле (6) уровню значимости $p = 0{,}01$. Это означает, что не произошло существенных изменений в распределении внутренних инцидентов в третьем квартале по сравнению со вторым.

Для сравнения рассмотрим внешние инциденты, т. е. инциденты, инициаторами и причиной которых становились действия лиц, не являющихся внутренними пользователями клиентов JSOC. Сводные частоты данных инцидентов приведены в табл. 4.

Таблица 4

Статистика по внешним инцидентам за третий и второй кварталы 2014 г.

Суммарные частоты инцидентов		Частоты инцидентов, связанных с реализацией типов угроз					
		E_1	E_2	E_3	E_4	E_5	E_6
		Атаки на веб-приложения	Brute-force и компрометация учетных данных внешних сервисов	Компрометация административных учетных записей	Атаки на управляющие протоколы систем	DDoS-атаки	Прочие внешние атаки
3 кв.	m	μ_1	μ_2	μ_3	μ_4	μ_5	μ_6
	7 166	2 723	1 835	100	373	215	1 920
2 кв.	n	ν_1	ν_2	ν_3	ν_4	ν_5	ν_6
	6 818	2 482	1 677	157	198	198	2 106

С помощью статистики χ^2 оценим, произошли ли изменения в распределении частот внешних инцидентов в третьем квартале по сравнению со вторым. По формуле (5) получим значение $\chi^2 = 85{,}23$ (для пяти степеней свободы). Оно значительно превышает критическое

значение $\chi^2_{5,p}$ = 15,09, которое согласно формуле (6) соответствует уровню значимости p = 0,01. Это означает, что отклонение от гипотезы об однородности распределений весьма значимо. Статистика показывает, что произошли существенные изменения в распределении внешних инцидентов. Отмечается смещение внешних атак на прикладной уровень. Одной из причин этого является существенное увеличение количества внешних ресурсов и веб-сервисов в компаниях практически всех отраслевых сегментов.

Предложенный метод носит универсальный характер и может использоваться для различных типов развертывания информационных систем (том числе для грид-систем) с целью выявления тенденций в динамике угроз. Действительно, если известны частоты инцидентов $\mu_1,\mu_2,...,\mu_i,...,\mu_r$ за текущий месяц, квартал, полугодие и при сравнении их с частотами инцидентов $\nu_1,\nu_2,...,\nu_i,...,\nu_r$ за прошлый год не выявлено существенного изменения в распределении вероятностей инцидентов (значение статистики χ^2 однородности не превышает заданного уровня), то с определенной вероятностью можно предположить, что эти показатели будут стабильны в среднесрочной перспективе. Это позволит спрогнозировать потенциальные частоты инцидентов $\eta_1,\eta_2,...,\eta_i,...,\eta_r$ на текущий год, которые, в свою очередь, могут быть использованы при оценке рисков ИБ.

Если же значение статистики χ^2 однородности значительно превышает заданный уровень, то необходимо выявлять причины сложившейся ситуации с изменением распределения инцидентов и проводить углубленный анализ угроз, воздействующих на систему.

Предлагаемый подход к анализу угроз ИБ позволяет провести оценку защищенности грид-системы, функционирующей в условиях воздействия рассматриваемого класса угроз, а также эффективности комплекса мероприятий и средств противодействия данным угрозам.

Заключение

На основании анализа опыта разработки распределенных вычислительных систем можно сделать вывод, что методы управления контролем безопасного доступа к услугам грид-систем должны обладать возможностями:

– осуществления однократной аутентификации пользователей;

– делегирования прав;

– интеграции с локальными системами безопасности и обмена политиками безопасности;

– обнаружения (предотвращения) угроз, вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к информации.

Угрозы безопасности информации в грид-системе определяются по результатам оценки и анализа возможных уязвимостей, способов реализации угроз безопасности информации и последствий от нарушения безопасности информации. Для оценки рисков ИБ рекомендуется использовать общедоступную базу данных CVE, банк данных ФСТЭК России (в особенности для государственных грид-систем), а также систему оценки общеизвестных уязвимостей CVSS и статистические критерии, в частности критерий χ^2.

Приоритетным направлением совершенствования средств и систем ИБ грид-систем является постепенный переход к созданию многоагентных систем защиты информации, реализующих централизованно-децентрализованный принцип построения, а также применение современных способов разграничения доступа к информации, в том числе на основе мультибиометрической аутентификации пользователей [10].

Список литературы

1. Информационная технология. Модель открытой грид-системы. Основные положения : ГОСТ Р 55768–2013. – М. : Стандартинформ, 2014. – 78 с.

2. О проблеме защиты информационных и вычислительных ресурсов в распределенных вычислительных сетях типа грид / М.О. Калинин [и др.] // XIV Санкт-Петербургская Междунар. конф. «Региональная информатика (РИ–2014)» : материалы конф. – СПб., 2014. – С. 553–554.

3. Information technology – Security techniques – Guidelines for the use and management of trusted third party services. ITU-T Recommendation X.842 (ISO/IEC TR 14516). – Montreal, 2000. – 35 p.

4. Сабанов, А.Г. О неизвлекаемости закрытых ключей / А.Г. Сабанов // Защита информации. Инсайд. – 2015. – № 2. – С. 30–33.

5. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности : СТБ 34.101.3–2014 (ISO/IEC 15408-3:2008). – Минск : Госстандарт, 2014. – 132 с.

6. Андреев, Д.С. Ритм набора парольной фразы как дополнительный признак аутентификации пользователя / Д.С. Андреев // Сб. науч. тр. IV Междунар. науч.-практ. конф. – Курск, 2014. – С. 68–74.

7. Старовойтов, В.В. Биометрические системы контроля доступа по отпечаткам пальцев / В.В. Старовойтов // Информатика. – 2015. – № 1. – С. 26–38.

8. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 16.01.2015 № 3 «О внесении дополнений и изменений в приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62» [Электронный ресурс]. – 2015. – Режим доступа : http://www.oac.gov.by/files/files/pravo/prikazi_oac/Prikaz_OAC_3.htm. – Дата доступа : 03.10.2015.

9. Методический документ. Меры защиты информации в государственных информационных системах (утвержден ФСТЭК России 11.02.2014) [Электронный ресурс]. – 2015. – Режим доступа : http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument. – Дата доступа : 03.10.2015.

10. Язов, Ю.К. Развитие информационных технологий и приоритетные направления исследований по совершенствованию защиты общих информационных ресурсов Беларуси и России в период 2016–2021 годов / Ю.К. Язов // Комплексная защита информации : материалы XX науч.-практ. конф., Минск, 19–21 мая 2015 г. – Минск : РИВШ, 2015. – С. 12–16.

11. Common Vulnerabilities and Exposures [Electronic resource]. – 2015. – Mode of access : http://www.cve.mitre.org. – Date of access : 30.07.2015.

12. Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю (ФСТЭК России) [Электронный ресурс]. – 2015. – Режим доступа : http://bdu.fstec.ru. – Дата доступа : 03.10.2015.

13. NVD Common Vulnerability Scoring System Support v.2 [Electronic resource]. – 2015. – Mode of access : http://www.nvd.nist.gov/cvss.cfm?calculator&version=2. – Date of access : 03.10.2015.

14. Система оценки общеизвестных уязвимостей. Рекомендация. МСЭ-Т X.1521 (04/2011) [Электронный ресурс]. – 2015. – Режим доступа : https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1521-201104-I!!PDF-R&type=items. – Дата доступа : 03.10.2015.

15. Трубей, А.И. Оценка рисков информационной безопасности с использованием существующей нормативной и методической базы / А.И Трубей // Информатика. – 2015. – № 2. – С. 102–114.

16. Vulnerability Severity Level [Electronic resource]. – 2015. – Mode of access : http://www.fortiguard.com/static/intrusionprevention.html. – Date of access : 03.10.2015.

17. Крамер, Г. Математические методы статистики / Г. Крамер. – М. : Мир, 1976. – 648 с.

18. JSOC Security flash report 2014 Q3 [Электронный ресурс]. – 2015. – Режим доступа : http://www.jet.msk.su/upload/content/jsoc-security-flash-report-q3-v-3.pdf. – Дата доступа : 03.10.2015.

Поступила 04.11.2015

Объединенный институт проблем
информатики НАН Беларуси,
Минск, Сурганова, 6
e-mail: trubeia@newman.bas-net.by

A.I. Trubei

ANALYSIS OF GRID-SYSTEMS INFORMATION SECURITY ASPECTS

The article presents the analysis of Grid-systems information security aspects, Also, risk assessment methods, using public databases, expert systems and statistical techniques are proposed.