автоматизированной станции и специальный блок программируемых реле, контакты которых показаны на рисунке. Команды на реле подаются с платы контроллера. Подключение электродвигателей к преобразователю или к сети производится реверсивными пускателями КМ1...КМ3, которые включаются через контакты реле. Применение реверсивных пускателей вызвано необходимостью защиты от попадания сетевого напряжения на выход преобразователя. Кнопочные посты S1...S4 позволяют включать насосные агрегаты вручную при выключенном электроприводе АТ, когда реле Кб выключено. Переключатели SA3...SA5 служат для выбора насосных агрегатов, включающихся автоматически при аварии преобразователя.

Программа управления реализована таким образом, что любой включаемый электродвигатель запускается плавно от преобразователя. При включении дополнительного насоса работающий от преобразователя агрегат переключается на работу от сети, а дополнительный подключается к выходу преобразователя и плавно разгоняется.

В состав САУ входят шкаф электропривода АТ04 со встроенным специальным технологическим субмодулем и силовые электрические аппараты коммутации и защиты. Шкаф электропривода АТ04 выполнен в обычном корпусе. Остальные элементы схемы, кроме датчика давления, размещаются в электрошкафу на объекте.

САУ, функционирующая в рамках иерархической АСУ ТП систем теплоснабжения получает информацию о задающих воздействиях по частоте вращения электродвигателей насосов.

Информационно-графическая система ТГИД-05, играющая роль системного интегратора на верхнем уровне АСУ, предназначенная для имитационного моделирования статических теплогидравлических режимов работы системы централизованного теплоснабжения, позволяет создавать и редактировать расчетные схемы, производить расчеты плановых и фактических теплогидравлических режимов, обладает мощным инструментарием анализа рассчитанных и измеренных параметров работы и в супервизорном варианте управления позволяет решать задачи в режимах разделенного и реального времени, связанные с выбором задающих воздействий для частотно управляемых электроприводов насосных станций каждой ветви теплоснабжающей сети с обеспечением в этих ветвях требуемых пьезометров.

УДК 004.056

САТЫБАЛДИНА Д.Ж.

Анализ уязвимостей информационных систем

В настоящее время с ростом количества угроз и уязвимостей проблема обеспечения информационной безопасности бизнеса становится всё актуальнее. В этих условиях руководство многих компаний сегодня приходит к тому, что система защиты информационных ресурсов должна строиться исходя из общепринятых норм и с учетом наработанных мировых практик, требований стандартов.

Одним из наиболее значимых международных стандартов в области информационной безопасности является стандарт ISO/IEC 17799, принятый также в Республике Казахстан [1]. В соответствии со стандартом ISO/IEC 17799 основное внимание при проектировании и создании эффективной системы безопасности организации уделяется комплексному подходу к управлению безопасностью. С целью формирования комплексных требований к безопасности информации стандарт определяет необходимость проведения оценки рисков, с которыми сталкивается организация (определение угрозы для ресурсов, их уязвимость и вероятность возникновения угроз, а также возможный ущерб). Именно поэтому выбор правильной методологии оценки угроз, а вместе с ними и уязвимостей информационной безопасности является актуальной проблемой, являясь одним из основных направлений при переходе к международным требованиям.

Ранее нами была разработана автоматизированная система «IT_Риск_Менеджер», предназначенная для построения моделей угроз, защиты от них, проведения анализа уязвимостей, возможных событий и оценки рисков в результате нарушений информационной безопасности [2-3]. В настоящей работе представлена концепция оценки уязвимостей различных программных и аппаратных платформ как один из этапов анализа и управления информационными рисками.

Так как уязвимостей, подлежащих категорированию, много, и они оценивались по разным шкалам, то сведение этих данных воедино для общего анализа является сложной проблемой. Общая система оценки уязвимостей (Common Vulnerability Scoring System, CVSS) предназначена для решения этой проблемы [4]. CVSS, разработанная Национальным институтом стандартов и технологий, совместно с Университетом Карнеги Мелоун, позволяет классифицировать известные и новые уязвимости согласно риску, который эти уязвимости представляют для компании и ее окружения.

Система оценки CVSS состоит из трех метрик: базовой, временной и контекстной. Каждая из метрик, в свою очередь, состоит из набора метрик.

Группа базовых метрик отображает характеристики уязвимости, которые не меняются со временем и не зависят от контекста. Метрики AccessVector (AV, Вектор доступа), AccessComplexity (AC, Сложность доступа) и Authentication (Au, Аутентификация) оценивают, как получить доступ к уязвимости и нужны ли для эксплуатации уязвимости дополнительные условия. Три метрики воздействия – Confidentiality Impact (C, Влияние на конфиденциальность), Integrity Impact (I, Влияние на целостность) и Availability Impact (A, Влияние на доступность) – описывают возможное прямое влияние на IT-систему в случае эксплуатации уязвимости. Это влияние определяется независимо с точки зрения конфиденциальности, це-

лостности и доступности. Это означает, например, что эксплуатация уязвимости может вызвать частичную потерю целостности и доступности, но не влиять на конфиденциальность.

Каждая метрика представляет собой оценку и значение в интервале от 0 до 10 и вектор – краткое текстовое описание со значениями, которые используются для вывода оценки.

Так, метрика AccessVector может принимать три значения Local (L), Adjacent Network (A), Network (N). В таблице 1 в качестве примера приведены её оценки и описания.

Таблица 1 – Оценка AccessVector

Значение метрики	Описание
Локальный (L)	Для эксплуатации уязвимости злоумышленник должен иметь локальный доступ, т.е. физический доступ к системе или локальную учетную запись.
Соседняя сеть (A)	Для эксплуатации уязвимости злоумышленник должен иметь доступ к соседней сети, т.е. такой сети, которая имеет общую среду передачи с сетью, где находится уязвимое ПО.
Сетевой (N)	Для эксплуатации уязвимости злоумышленник должен обладать доступом к уязвимому ПО, причем этот доступ ограничен только величиной сетевого стека. Локального доступа или доступа из соседней сети не требуется. Такие уязвимости часто называют эксплуатируемыми удаленно.

Спектр возможной сложности доступа (AccessComplexity) также расширен: High (H), Med (M), Low (L). Возможные значения аутентификации (Authentication) включают Multiple (M), Single (S) и None (N).

Временные метрики и контекстные являются необязательными, они не влияют на базовую оценку. Эти метрики применяются только в тех случаях, когда пользователь хочет уточнить базовую оценку. Три фактора, которые изменяются со временем и учитываются в CVSS: Exploitability (E, Возможность использования), Remediation Level (RL, Уровень исправления), Report Confidence (RC, Степень достоверности отчета).

Группа контекстных метрик CVSS отражает характеристики уязвимости, которые связаны со средой пользователя: Collateral Damage Potential (CDP, Вероятность нанесения косвенного ущерба), Target Distribution (TD, Плотность целей) и Security Requirements (CR, IR, AR, Требования к безопасности).

Каждая метрика в соответствующем векторе представлена сокращенным именем метрики, за которым следует ":" (двоеточие), а затем – сокращенное значение метрики. Вектор содержит последовательность метрик в заранее заданном порядке, при этом символ "/" (слеш) используется для разделения метрик. Если временная или контекстная метрика не используется, то проставляется значение "ND" (не определено). Базовый, временной и контекстный векторы представлены в таблице 2.

Базовая формула оценки уязвимостей имеет следующий вид (версия 2.10):

BaseScore = round_to_1_decimal (((0.6*Impact)+
+(0.4*Exploitability)-1.5)*f(Impact)),

где

Impact = 10.41*(1-(1-ConfImpact)+
+*(1-IntegImpact)*(1-AvailImpact)),

Exploitability = 20*AccessVector*
*AccessComplexity*Authentication,

f(Impact) = 0 if Impact = 0, 1.176 otherwise

AccessVector = case AccessVector of
requires local access: 0.395
adjacent network accessible: 0.646
network accessible: 1.0

AccessComplexity = case AccessComplexity of
high: 0.35
medium: 0.61
low: 0.71

Authentication = case Authentication of
requires multiple instances of authentication: 0.45
requires single instance of authentication: 0.56
requires no authentication: 0.704

ConfImpact = case ConfidentialityImpact of
none: 0.0
partial: 0.275
complete: 0.660

IntegImpact = case IntegrityImpact of
none: 0.0
partial: 0.275
complete: 0.660

AvailImpact = case AvailabilityImpact of
none: 0.0
partial: 0.275
complete: 0.660

При использовании временной формулы временные метрики объединяются с базовыми, чтобы вывести временную оценку в интервале от 0 до 10. Временная оценка не превышает базовую и не более чем на 33% меньше ее. При использовании контекстных формул контекстные метрики объединяются с временными метриками, чтобы получить оценку окружения в интервале от 0 до 10. Значение контекстной метрики, полученное из этой формулы, не должно превышать временную оценку.

Таблица 2 – Базовый, временной и контекстный вектор

Название метрики	Описание
Базовый	AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
Временной	E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]
Контекстный	CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/ IR:[L,M,H,ND]/AR:[L,M,H,ND]

В качестве примера в руководстве [4] рассмотрена уязвимость CVE-2003-0818: уязвимость при обработке целочисленных значений в библиотеке Microsoft Windows ASN.1. Уязвимость была обнаружена в сентябре 2003 года и касается библиотек ASN.1 во всех операционных системах Microsoft. Удачная эксплуатация этой уязвимости приводит к переполнению буфера, что позволяет злоумышленнику выполнить произвольный код с привилегиями администратора.

Эта уязвимость эксплуатируется удаленно и не требует аутентификации, поэтому Access Vector равен «Network» и «Authentication» равен «None». Access Complexity имеет значение «Low», потому что дополнительный доступ или специальные условия не требуются для эксплуатации этой уязвимости. Каждая из метрик Impact имеет значение «Complete», потому что существует возможность полной компрометации системы. Эти метрики вместе дают максимальное значение базовой оценки 10.0.

Базовый вектор данной уязвимости: AV:N/AC:L/Au:N/C:C/I:C/A:C. Все оценки представлены в таблице 3.

Таблица 3 – Оценки и значения базовых метрик для уязвимости CVE-2003-0818

Базовая метрика	Оценка	Значение
Access Vector	[Network]	(1.00)
Access Complexity	[Low]	(0.71)
Authentication	[None]	(0.704)
Confidentiality Impact	[Complete]	(0.66)
Integrity Impact	[Complete]	(0.66)
Availability Impact	[Complete]	(0.66)

Вычисление базовой оценки дает следующий результат:

$$\text{Impact} = 10.41*(1-(1-0.66)+*(1-0.66)*(1-0.66)) = 10.0,$$

$$\text{Exploitability} = 20*1*0.71*0.704 = 9.99 = 10,$$

$$f(\text{Impact}) = 0, 1.176$$

$$\text{BaseScore} = \text{round\_to\_1\_decimal}\ (((0.6*10.0)+ +(0.4*10.0)-1.5)*1.176)) = 10.0,$$

Получено максимальное значение базовой оценки 10.0.

Для этой уязвимости существуют эксплойты, поэтому Exploitability имеет значение «Functional». Microsoft выпустила исправление MS04-007 в феврале 2004 года, поэтому Remediation Level имеет значение «Official-Fix» и Report Confidence имеет значение «Confirmed». Эти метрики позволяют скорректировать базовую оценку и получить временную оценку 8.3.

Приняв, что доступность менее важна, чем обычно для целевых систем, и опираясь на значения Collateral Damage Potential и Target Distribution, оценка окружения изменяется в пределах от 0.0 («None», «None») до 9.0 («High», «High»).

Концепция CVSS является понятным, прозрачным и общепринятым способом оценки уязвимостей. Использование доступного математического аппарата в автоматизированной системе «IT_Риск_Менеджер» позволило получить корректные количественные оценки уязвимостей. В программе предусмотрено дополнительное применение сканера или технологии мониторинга, чтобы определить наличие уязвимости в сетевом или локальном приложении. Затем эти данные объединяют с базовой, временной и контекстной оценками CVSS, чтобы получить информацию, наиболее полно отражающую риск в данном контексте, и исправить именно те уязвимости, которые представляют наибольшую опасность для информационных систем.

СПИСОК ЛИТЕРАТУРЫ

1. СТ РК ИСО/МЭК 17799-06 (ИСО/МЭК 17799-2005, IDT). Информационная технология. Методы обеспечения защиты. Свод правил по управлению защитой информации.
2. Сатыбалдина Д.Ж., Холявко А.А. Методы и средства управления рисками// Сб. трудов Второй междунар. науч.-практ. конф. «Проблемы инновационного развития нефтегазовой индустрии». Алматы, 26-27 февраля 2009. Алматы, 2009. С. 94-98.
3. Сатыбалдина Д.Ж. Проектирование автоматизированной системы управления информационными рисками // Вестник ВКГТУ им. Д. Серикбаева. 2009. №4. С. 173-179.
4. Peter Mell, Karen Scarfone, Sasha Romanosky. A Complete Guide to the Common Vulnerability Scoring System. Version 2.0. 2007. 23 pp.