Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

инциденты – определяются на основе методов, тактик и процедур анализа на базе опыта SOC по реагированию на киберинциденты;

другие наборы данных – это данные, полученные от сбора, аналитической обработки и научно-исследовательской деятельности.

Предлагаемое решение проблемы конфиденциальности данных, не покидающих границы страны:

развертывание оборудования на предприятии заказчика;

поддержка частично децентрализованных сервисов на ресурсах национального партнёра;

хранение данных журналов протоколирования и конфигурирования на устройствах в стране под контролем заказчика;

передача только мета-данных (подмножества полного журнала) в зарубежный SOC, чтобы позволить генерировать сигналы тревоги и вызывать принятие различных действий для реагирования.

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ СТАНДАРТА CVSS 3.0

М.Н. БОБОВ, Д.Г. ГОРЯЧКО

ОАО «АГАТ-системы управления» – управляющая компания холдинга «Геоинформационные системы управления»

Оценка риска информационной безопасности в общем случае определяется как комбинация вероятности угрозы и ущерба от её реализации [1].

$$R_o = P * D,$$

где R_o – показатель риска,

P – оценка вероятности реализации угроз безопасности,

D – показатель ущерба.

Последовательность выполнения работ по оценке риска показана на рисунке 1.

Как видно из рисунка оценка вероятности реализации угроз безопасности P_{vi} определяется соотношением:

$$P_{vi} = F(f_{vi}, Vul), \quad (1)$$

где f_{vi} – оценка частоты воздействия источников угроз;

Vul – оценка уязвимостей (условий реализации угроз).

Оценка частоты воздействия источников угроз f_{vi} и оценка уязвимостей Vul в настоящее время осуществляется на основе использования экспертных методов. Существует ряд систем оценки уязвимостей, которые созданы коммерческими и некоммерческими организациями, в том числе CERT/CC, системы анализа уязвимостей SANS и Microsoft. Однако, на наш взгляд, наиболее подходящим средством оценки уязвимостей для определения риска информационной безопасности эксплуатируемых информационных автоматизированных систем является стандарт CVSS [2].

В стандарте используются три показателя оценки уязвимостей:
B – базовый; T – временной; E_n- локализованный.

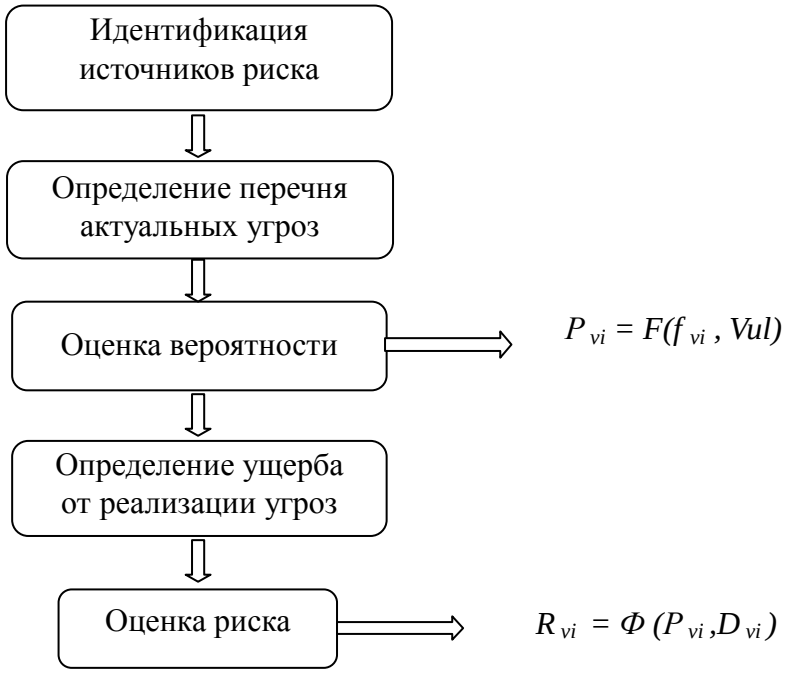

Рис. 1 – Последовательность выполнения работ по оценке риска

Базовый показатель B является основным и отражает сущностные свойства уязвимости, не зависимо от времени её существования и среды эксплуатации. Временной *T* и локализованный E_n показатели уточняют базовый показатель в зависимости от того, какие меры были предприняты по уменьшению влияния уязвимости с момента её обнаружения и какие возможности по её использованию предоставляет конкретная среда функционирования. Для оценки уязвимостей в конкретных эксплуатируемых системах необходимо использовать локализованный показатель уязвимости E_n, который является функцией базового и временного показателей:

$$E_n = f(T,B)$$

Базовый показатель определяется в соответствии с формулой (2) и является функцией ниже перечисленных параметров.

$$\boldsymbol{B} = \boldsymbol{F}(AV,AC,PR,UI,C,I,A), \quad (2)$$

где AV – вектор атаки, **AC** – сложность атаки, **PR** – требуемые привилегии, **UI** – участие пользователя, влияние на уровень конфиденциальности, целостности и доступности – **C, I, A I**mpact.

Временной показатель определяется на основе базового показателя **B** по формуле (3) и является функцией приведенных ниже дополнительных параметров.

$$T = \Phi(B, ECM,RL,RC), \quad (3)$$

где **ECM** – степень зрелости кода эксплойта, **RL** – уровень исправления, RC – **с**тепень достоверности отчёта.

И, наконец, требуемый локализованный показатель является функцией временного параметра и дополнительных показателей CR, IR, AR, а именно:

$$E_n = f(T, CR, IR, AR), \qquad 0 < E_n < 10,$$

где **CR IR AR** – требования по конфиденциальности, целостности и доступности к объекту, содержащему уязвимость.

В стандарте определены числовые значения параметров, используемых при оценке показателей уязвимости, приведенные ниже в таблицах 1 и 2.

На основе значений параметров, приведенных в таблицах 1 и 2, построены графики показателя E_n в зависимости от степени зрелости кода эксплойта и уровня исправления кода объекта, содержащего уязвимость, для фиксированных параметров вектора атаки – $E_N = F_{AV}(ECM)$ и $E_N = F_{AV}(RL)$. Полученные графики показывают линейный характер изменения показателя E_N при изменении значений параметров ECM и RL для групп максимального и минимального значения параметров базового показателя **B**.

Таблица 1 – Числовые значения параметров

Параметр	Оценка	Числовое значение
Вектор атаки – **AV**	Network	0.85
	Adjacent Network	0.62
	Local	0.55
	Physical	0.2
Сложность атаки – **AC**	Low	0.77
	High	0.44
Требуемые привилегии – **PR**	None	0.85
	Low	0.62
	High	0.27
Участие пользователя – **UI**	None	0.85
	Required	0.62
Влияние на уровень конфиденциальности, целостности и доступности – **C, I, A** Impact	High	0.56
	Low	0.22
	None	0

Поскольку базовая и временная оценки уязвимостей и векторы CVSS публикуются в свободно распространяемых бюллетенях безопасности, это позволяет оперативно проводить оценку рисков информационной безопасности действующих систем в реальных условиях эксплуатации. Кроме того, в этих документах содержится много полезной для анализа информации, включая дату обнаружения уязвимости, системы, которые ей подвержены, и ссылки на производителей для поиска информации об исправлении.

Оценка частоты воздействия источников угроз также производится экспертами и может принимать значения [3]:

2 – для значения «крайне редко»;

4 – для значения «редко»;

6 – для значения «регулярно»;

8 – для значения «часто»;

10 – для значения «очень часто».

Параметр	Оценка	Числовое значение
Степень зрелости кода эксплойта – **ECM**	Not Defined	1
	High	1
	Functional	0.97
	Proof of Concept	0.94
	Unproven	0.91
Уровень исправления – **RL**	Not Defined	1
	Unavailable	1
	Workaround	0.97
	Temporary Fix	0.96
	Official Fix	0.95
Степень достоверности отчёта – **RC**	Not Defined	1
	Confirmed	1
	Reasonable	0.96
	Unknown	0.92
Требования по конфиденциальности, целостности и доступности – **CR, IR, AR**	Not Defined	1
	High	1.5
	Medium	1
	Low	0.5

Оценка вероятности реализации угроз безопасности (P) на основании формулы (1) может быть определена соотношением:

$$P = f_{vi} * Vul /100, \quad 0 < P < 1$$

В заключение необходимо отметить, что многие производители приложений также предоставляют базовые оценки CVSS и векторы своим клиентам. Это позволяет пользователям иметь объективную информацию о продуктах и даёт возможность эффективно управлять IT-рисками.

Список литературы

1. Бобов, М.Н. Оценка рисков информационной безопасности автоматизированных систем / М.Н. Бобов, Д.Г. Горячко, А.А. Обухович // Информационно-измерительные и управляющие системы. 2016. – №4, т. 14. – С. 69-74.

2. Common Vulnerability Scoring System v3.0: Specification Document. – Режим доступа- https://www.first.org/cvss.

3. Бобов, М. Н. Методология оценки рисков информационной безопасности / М.Н. Бобов, А.А. Обухович // XVIII научно-практическая конференция «Комплексная защита информации» : тезисы докл. – Брест, 2013.