DOI: 10.25728/mlsd.2023.1227

КОМПЛЕКСНОЕ ОЦЕНИВАНИЕ ИНФОРМАЦИОННЫХ РИСКОВ ИНТЕРНЕТА ВЕЩЕЙ: ОЦЕНКА КОНФИДЕНЦИАЛЬНОСТИ

Рей А. С.
Институт проблем управления им. В.А. Трапезникова РАН, Москва, Россия
a.rey@ipu.ru

Аннотация. Представленная работа посвящена использованию механизма комплексного оценивания с целью оценки уровня безопасности Интернета вещей путем анализа информационных рисков. В работе предлагается метод оценки конфиденциальности системы как компонента интегрального информационного риска. В работе описана сам метод и приведены примеры возможных шкал и значений критериев комплексного оценивания.

Ключевые слова: информационный риск, интернет вещей, конфиденциальность, механизмы комплексного оценивания.

Введение

В настоящее время специалисты и исследователи отмечают недостаток в уровне безопасности SMART-систем на базе Интернета вещей [1]. В связи с этим возникает необходимость в совершенствовании методов оценки рисков, с целью обеспечения их безопасности.

Под информационным риском будет пониматься наступление такого события (атаки), при котором происходит непосредственное воздействие на информацию системы. Согласно [2], уровень защиты системы оценивается по критериям конфиденциальности, целостности и доступности информации. В данной работе предлагается подход для решения задачи оценки конфиденциальности SMART-систем на базе Интернета вещей путем адаптации метода комплексного оценивания (КО).

1. Оценка информационных рисков: оценка конфиденциальности

В работе [3] отмечается, что интегральный информационный риск складывается из совокупности локальных рисков, какими могут служить риски по утрате конфиденциальности, целостности или доступности, как характеристики информационной безопасности. Кроме того, оценка информационного риска обычно является качественной, а количественные оценки строят лишь в редких случаях. Автор также отмечает, что оценка носит субъективный характер, так как производится экспертами. Однако, предложенный автором общий подход по оценке интегрального информационного риска, не дает решения, как оценивать каждую характеристику по отдельности.

В настоящей работе предлагается использовать механизмы КО [4]. Несмотря на то, что механизм КО является экспертным (параметры оценивания, включая структуру бинарного дерева свёртки критериев, значения критериев и шкалы их оценивания, верхние и нижние границы возможного диапазона риска формируются экспертами), он обладает свойством неманипулируемости при использовании анонимной медианной схемы согласования [5], что обеспечивает устойчивость комплексной оценки в условиях расхождений мнений экспертов. Мы рассмотрим способ оценки одного из локальных информационных рисков, — конфиденциальности — что позволит в дальнейшем оценить уровень безопасности системы в целом. В качестве предмета будем рассматривать систему Интернета вещей.

Оценку проводим следующим образом: сначала для оценки уровня безопасности и защищенности Интернета вещей от утраты конфиденциальности информации будем строить матрицу влияния типичных атак (см., например, [6, 7]) на конфиденциальность системы. В ходе анализа было установлено, что на конфиденциальность Интернета вещей влияют следующие виды атак (таблица 1):

Таблица 1. Перечень атак, влияющих на конфиденциальность Интернета вещей

An	**Виды атак**	**Комментарии**
A1	Заражение	Вредоносное ПО, программы вымогатели, вредоносные устройства, вредоносный код, заражение трояном
A2	Подслушивание	Прослушивание, сканирование, сбор голосовых данных
A3	Кража данных	Фишинг
A4	Перенаправление	Спуфинг (IP - , MAC - ,DNA -), имперсонация, атака посредника
A5	Подбор	Подбор ключа путем перебора всех возможных вариантов (Brute-force), перебор по словарю

An	Виды атак	Комментарии
A6	Атака по сторонним каналам	Анализ мощности, атака по времени, атака по ошибкам вычисления

На следующем шаге требуется определить, какие уязвимости характерны для системы в целом. В обзорной литературе можно часто встретить перечень основных уязвимостей для Интернета вещей (таблица 2):

Таблица 2. Перечень распространённых уязвимостей Интернета вещей

Yn	Уязвимости	Источник
У1	Гетерогенная архитектура	[7]
У2	Недостаточная физическая безопасность	[6]
У3	Ненужные открытые порты	[6]
У4	Устаревшие протоколы	[7]
У5	Слабое шифрование	[6, 7]
У6	Небезопасные приложения	[7]
У7	Недостаточный контроль доступа	[6]
У8	Плохая аутентификация	[6, 7]
У9	Слабые методы программирования	[6]
У10	Неправильная возможность обновления ПО	[6, 7]
У11	Недостаточные механизмы аудита	[6]

Следующий шаг заключается в определении того, какими уязвимостями могут воспользоваться злоумышленники для проведения той или иной атаки. В таблице 3 приведена матрица зависимости возможности реализации атак от наличия в системе тех или иных уязвимостей. На вертикальной оси указан перечень атак, проведение которых может повлиять на нарушение конфиденциальности Интернета вещей (см. табл. 1), а на горизонтальной оси указаны распространенные уязвимости Интернета вещей (см. табл. 2). На пересечении осей отмечено при каких уязвимостях возможно осуществление конкретных атак. Обратим внимание, что в нашем примере, мы рассматриваем случаи, когда атаки осуществляются не последовательно, а вариативно.

Четвертым шагом является построение рейтинга. Проранжируем атаки в соответствии с числом задействованных уязвимостей. Ранг 1 присваивается атаке (или атакам), возможность реализации которой зависит от наибольшего числа уязвимостей, ранг 2 — атакам, эксплуатирующим наибольшее число уязвимостей, за исключением атак с ранее присвоенным рангом 1, и так далее. Результаты представлены в колонке «Ранг» таблицы 3.

Таблица 3. Сопоставление уязвимостей и атак

Атаки	Уязвимости											Ранг
	У1	У2	У3	У4	У5	У6	У7	У8	У9	У10	У11	
A1	**V**		**V**	**V**	**V**	**V**		**V**	**V**	**V**	**V**	1
A2	**V**	**V**	**V**	**V**	**V**		**V**		**V**		**V**	2
A3				**V**	**V**		**V**	**V**	**V**		**V**	3
A4	**V**			**V**	**V**	**V**					**V**	4
A5					**V**			**V**				5
A6		**V**			**V**							5

Следующим шагом будет построение бинарного дерева оценки свёртки критериев оценки конфиденциальности (рисунок 1). Листьями дерева будут критерии, соответствующие рискам успешного осуществления атак, перечисленных в таблице 1. Для свертки в нашем примере будем выбирать те атаки, что используют минимум одну общую уязвимость. Если два листа соответствуют атакам с равным рангом, будем осуществлять их свёртку по обычным правилам (см. [4]). В случае, если таких атак три или больше, для свёртки будем использовать метод порогового агрегирования [8]. При таком способе построения длина простой цепи, соединяющей корень дерева с листом будет соответствовать рангу представляемой им атаки.

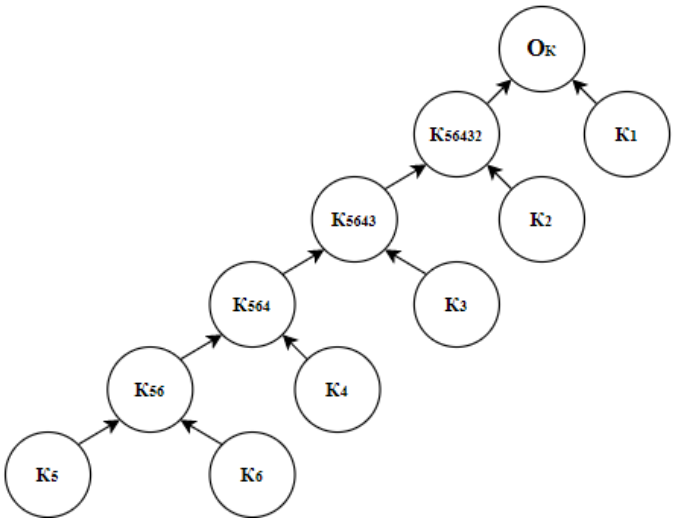

Рис. 1. Бинарное дерево для оценки конфиденциальности Интернета вещей

2. Пример расчёта показателя «оценка конфиденциальности» Интернета вещей

Следующим шагом, после построения бинарного дерева, будет определение шкал и значений оценки критериев. В данном случае была выбрана единая шкала оценивания как критериев уровней риска осуществления атаки, так и синтетических критериев. Нами была введена 5-балльная шкала, где

- 1 – очень высокий риск осуществления атаки;
- 2 – высокий риск осуществления атаки;
- 3 – средний риск осуществления атаки;
- 4 – низкий риск осуществления атаки;
- 5 – риск осуществления атаки отсутствует.

В данном случае, значения показателей дискретной шкалы определяются в зависимости от наличия в системе противодействующих мер [6] и дискретная шкала со значениями для оценки каждого показателя имеет следующий вид (таблица 4):

Таблица 4. Дискретная шкала со значения оценки для каждого показателя

Крите рии	**Хар-ка критериев**	**Значение дискретной шкалы**	
К6	Риск осуществлен ия атаки по сторонним каналам	1	отсутствуют средства защиты от атаки по сторонним каналам, отсутствуют ограничения на физический доступ к устройствам
		2	только ограничения на физический доступ к устройствам
		3	установлена 1 мера защиты из п.5
		4	установлены 2-3 меры защиты из п.5
		5	установлены меры защиты: генератор шума, управление временем выполнения операций, баланс энергопотребления, маскировка промежуточных вычислений, шифрование вычислений, ограничения физического доступа к устройствам
К5	Риск осуществлен ия атаки подбора	1	пароль отсутствует или очень слабый, отсутствуют ограничения по вводу пароля
		2	надежный пароль, но отсутствуют др. методы защиты
		3	надежный пароль, мульти-факторная аутентификация

Критерии	Хар-ка критериев	Значение дискретной шкалы	
		4	надежный пароль, мульти-факторная аутентификация, биометрия
		5	надежный пароль, мульти-факторная аутентификация, биометрия, распределенный доступ, наличие нескольких уровней хранения данных, настроенный брандмауэр, подключены контрольные, технические, рисковые фреймворки
К4	Риск осуществления атаки перенаправления	1	все критерии из п.5 отсутствуют
		2	наличие только динамической проверки ARP
		3	наличие только одного компьютера и интерфейса маршрутизатора в одном VLAN, динамической проверки APR
		4	наличие: только одного компьютера и интерфейса маршрутизатора в одном VLAN, протоколов шифрования данных, измерений уровня сигнала и оценки канала связи; использование секретного ключа для длительного сеанса, контроля протоколов, учтены все критерии модели безопасности гетерогенной архитектуры, есть журналы учета трафика. Отсутствует регулярность обновления приложений
		5	наличие только одного компьютера и интерфейса маршрутизатора в одном VLAN, протоколов шифрования данных, спам-фильтров, регулярно обновляемых приложений, измерений уровня сигнала и оценки канала связи, журналы учёта трафика; использование секретного ключа для длительного сеанса; контроль протоколов, распределения энергии; соблюдены все критерии модели безопасности гетерогенной архитектуры
К3	Риск осуществления атаки кражи данных	1	все критерии из п.5 отсутствуют
		2	отсутствует 3 - 4 критерия из п. 5
		3	отсутствуют 2 критерия из п.5
		4	отсутствует 1 критерий из п.5
		5	наличие фильтрации URL-запросов, спам-фильтров, антивирусов, брандмауэра, протоколов шифрования данных, использование криптоалгоритмов защиты IP-Потока, шифрования трафика, межсетевых экранов, шифрования вычислений, использование защищенных протоколов
К2	Риск осуществления атаки подслушивания	1	все критерии из п.5 отсутствуют
		2	отсутствует 3 - 4 критерия из п. 5
		3	отсутствуют 2 критерия из п.5
		4	отсутствует 1 из критериев п.5
		5	использование криптоалгоритмов защиты IP-Потока, защищенных протоколов, систем обнаружения вторжений и уязвимостей, сканеров портов и средств выявления топологии сети; наличие высоких требований к физическому доступу к аппаратам, шифрования трафика
К1	Риск осуществления атаки заражения	1	все критерии из п.5 отсутствуют
		2	отсутствует 3 - 4 критерия из п. 5
		3	отсутствуют 2 критерия из п.5
		4	отсутствует 1 из критериев п.5
		5	соблюдены все критерии модели безопасности гетерогенной архитектуры, осуществляется контроль протоколов, есть журнал трафика, присутствуют спам-фильтры, происходит регулярное обновления ПО и приложений, наличие протоколов шифрования данных, мульти-факторной аутентификации, антивирусов, межсетевых экранов, шифрования вычислений, использование защищенных протоколов

Заключительным шагом оценки конфиденциальности системы является анализ системы Интернета вещей и построение матриц свёртки на основе проделанного анализа. В нашем случае мы получили матрицы следующего вида (рисунок 2). Присвоив критерию **К5** (риск осуществления атаки подбора) оценку **3**, критерию **К6** (риск осуществления атаки по сторонним каналам) тоже оценку **3**, мы получили синтетический критерий **К56 = 3**. Присвоив критерию **К4** (риск осуществления атаки перенаправления) оценку **2**, получаем синтетический критерий **К564 = 2**. Если оценка критерия **К3** (риск осуществления атаки кражи данных) = **3**, то критерий **К5643 = 2**. В таком случае, когда критерий **К2** (риск осуществления атаки кражи данных) = **2**, критерий **К56432** тоже = **2**. Таким образом, если критерий **К1**

(риск осуществления атаки подслушивания) = **3**, то в результате сворачивания матриц по правилам (см. [4]) получаем оценку конфиденциальности Интернета вещей. В конкретном примере оценка конфиденциальности = **2**, что равнозначно высокому риску осуществления атак, нарушающих такой аспект информационной безопасности, как конфиденциальность.

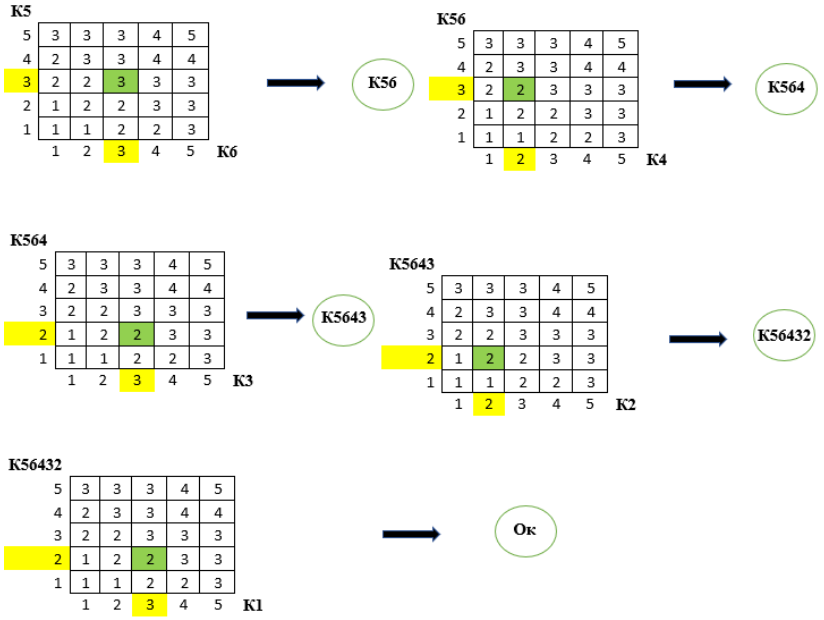

Рис. 2. Пример свёрточных матриц оценки конфиденциальности

3. Заключение

Конфиденциальность является одним из основных аспектов информационной безопасности. В работах других авторов были предложены решения для общей оценки информационных рисков. В данной же работе предлагается способ оценки отдельной характеристики информационной безопасности, на примере системы Интернета вещей.

Предложенная оценка состоит из семи этапов, где на первом этапе – определяются атаки, характерные для Интернета вещей и влияющие на нарушение конфиденциальности, на втором – выделяются возможные уязвимости Интернета вещей, на третьем этапе – атаки сопоставляются с уязвимостями, в которые они бьют, на четвертом этапе – проводится ранжирование атак в зависимости от количества, сопоставимых на предыдущем этапе, уязвимостей, на пятом – строится бинарная структура, где листьями одного уровня будут те атаки, что задействуют как минимум одну уязвимость, на шестом этапе – определяются шкалы и их значения, а на заключительном этапе – анализируется система, строится матрица свёртки и вычисляется критерий «оценка конфиденциальности».

Стоит отметить, что данная работа не рассматривает другие варианты ранжирования атак, например случаи, когда атаки реализуются не вариативно, а последовательно, где следует учитывать важность уязвимостей. В работе также не рассмотрены случаи неопределенности, когда, например, один критерий влияет на другой. Помимо этого, в работе не представлены варианты, когда у атак отсутствуют общие уязвимости.

Тем не менее, описанная оценка позволяет вычислить один локальный риск, тем самым решая проблему по оценке конфиденциальности системы. В дальнейшем этот подход можно использовать при общей оценке безопасности информационной системы.

Литература

1. *Abiodun O.I., Abiodun E.O., Alawida M. et al.* A Review on the Security of the Internet of Things: Challenges and Solutions // Wireless Personal Communications. – 2021. – Vol. 119, N 1. – P. 2604–2637.
2. *ГОСТ Р ИСО/МЭК 27002-2021* Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности // Официальное издание. М.: Стандартинформ, 2021
3. *Калашников А.О.* Управление информационными рисками организационных систем: механизмы комплексного оценивания // Информационная безопасность. – 2016. – Т. 3, № 1. – С. 315–322.

4. *Баркалов С.А.* Модели управления конфликтами и рисками: монография / С.А. Баркалов, Д.А. Новиков, В.И. Новосельцев и др. – под ред. Д.А. Новикова – Воронеж: Научная книга, 2008. – 495 с.
5. *Алексеев А.О.* Исследование устойчивости механизмов комплексного оценивания к стратегическому поведению агентов (на примере согласования политики организации в области риск-менеджмента) // Прикладная математика и вопросы управления. – 2019. – № 4. – С. 136–154.
6. *Neshenko N., Bou-Harb E., Crichigno J., Kaddoum G., Ghani N.* Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations // IEEE Communications Surveys & Tutorials. – 2019. – Vol. 21, N 3. – P. 2702–2733.
7. *Abdullah A.A., Waleed A., Malebary S., Adel A.A.* A review of cyber security challenges attacks and solutions for Internet of Things based smart home // Int. J. Comput. Sci. Netw. Secur. – 2019. – Vol. 9, N 9. – P. 139–146.
8. *Алескеров Ф.Т., Якуба В.И.* Метод порогового агрегирования трехградационных ранжировок // Доклады академии наук. – 2007. – Т. 413, № 2. – С. 181–183.