УДК 004.05

Рагимов Э.Р.
Институт Информационных Технологий НАНА, Баку, Азербайджан
elshan_rahimoff@mail.ru

КВАЛИМЕТРИЧЕСКИЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ ПРОГРАММНЫХ КОМПЛЕКСОВ, РЕАЛИЗУЮЩИХ СИСТЕМУ УПРАВЛЕНИЯ КОРПОРАТИВНЫМИ СЕТЯМИ

Статья посвящена вопросам определения квалиметрических показателей безопасности программных комплексов, которые выполняют основную роль системы управления корпоративными сетями. С помощью определения качественных характеристик показана возможность выявления первичных элементов безопасности. На основе данного подхода был разработан механизм выявления надежности квалиметрических данных безопасности программного комплекса.

Ключевые слова: *безопасность, отказ, система защиты информации, программный комплекс, корпоративная сеть, квалиметрические показатели.*

1. Введение

В центре управления различными, географически распределенными крупномасштабными проектами стоит система управления корпоративными сетями, которая в свою очередь состоит из взаимосвязанных программных модулей. Роль отдельных программных средств, которые в совокупности составляют программные комплексы, весьма удельна в общей системе управления корпоративными сетями (КС). Одной из базисных точек управления КС является система защиты информации, циркулирующей в ней. Реализация успешной системы защиты информации КС напрямую связана с безотказной и безопасной работой программных комплексов, что и является качественным показателем. Безопасность каждого программного модуля, включенного в программный комплекс, реализующий общую систему защиты информации КС, так же важна, как и безопасность всей системы в целом. При такой ситуации соответственно интерес к программным средствам, их реализации, применению и безопасности на сегодняшний день весьма возрастает. Так как основной груз реализации и управления защитой информации КС лежит на программных средствах, то безопасность самих средств должна быть определена на более ранних этапах проектирования корпоративных сетей. Разновидность требований, предъявляемых к программным средствам, реализующим систему управления КС, привела к стремительному развитию внутренней архитектуры, появлению методов реализации и спектров сервисов, предоставляемых программными средствами, что в свою очередь усложнило оценивание безопасности программных комплексов [1]. Также реализация того или иного программного комплекса в системе управления КС на более ранних этапах проектирования сопровождается появлением элементов неопределенности и непредсказуемости, так как разновидность программных комплексов является самой главной причиной неопределенности. Принимая во внимание вышеизложенное, возможно сформулировать, что измерение качества реализации безопасности программных комплексов составляет основную линию безопасности управления КС в целом. Данная статья посвящена определению квалиметрических данных (измерений качественных показателей) безопасности программных комплексов, реализующих систему управления КС.

2. Основы квалиметрических показателей безопасности

Привилегия применения измерений качественных показателей в априорных элементах безопасности решает ряд вопросов, как административных, так и финансовых, так как весьма широкая разновидность программных комплексов, выполняющих систему управления КС, ведет при проектировании КС к сложности принятия решений выбора того или иного программного комплекса. Особенно с учетом того, что при такой разнообразной палитре программных комплексов также немаловажную роль играет финансовый вопрос, ведь в зависимости от предлагаемых услуг и производителя стоимость программных комплексов меняется. Выявление квалиметрических показателей безопасности программных комплексов создает возможность при реализации широкомасштабных проектов на основе распределенной структуры КС владеть количественными оценками качества первичных показателей безопасности. На сегодняшний день на практике широкое применение нашел экспертный метод квалиметрии, но так как в процессе оценивания существует субъективное мнение, данный подход нуждается в доработке [2, 3]. Для получения более точных результатов рекомендуется принять во внимание следующие аспекты:

– Для каждого измерительного процесса в зависимости от функциональных возможностей программного комплекса алгоритм экспертного метода и систему показателей, характеризующих качество эксперта, нужно варьировать.

– Существование возможности применения математических методов для выявления требуемой численной оценки показателей безопасности.

– Существование возможности для более детальной или словесной характеристики априорных показателей безопасности программных комплексов для точного анализа экспертов.

– Вне зависимости от стадии эксплуатации системы управления КС должна существовать возможность частичного или полного комбинирования групп экспертов, работающих в разных направлениях оценивания безопасности системы управления КС в целом. Также возможность определения оптимального количества экспертов в составе одной рабочей группы должна быть соблюдена на более ранних этапах проектирования системы управления КС. При принятом экспертами финальном заключении учитывание роли каждого эксперта в комбинированной экспертной группе занимает центральное место. Что в свою очередь возможно сформулировать так:

$$K_i^{комб} = \frac{1}{N_j} \left(\sum_{j=1}^{N_j} K_{ij} V_{ij}\right), \qquad (1)$$

где $K_i^{комб}$ – экспертная оценка комбинированной экспертной группы, значение данного параметра меняется в интервале [0,1]; K_{ij} – экспертная оценка одиночного эксперта в составе комбинированной группы, значение данного параметра меняется в интервале [0,1]; N_j – количество экспертов в комбинированной группе; i – количество экспертных подгрупп в составе комбинированной группы; V_{ij} – коэффициент весомости j-го эксперта в составе комбинированной группы.

Следует также определить зависимость между коэффициентом весомости и экспертной достоверностью D_{ij}:

$$V_{ij} = \frac{1}{(1-D_{ij})^2 \sum_{j=1}^{N_i} \frac{1}{(1-D_{ij})^2}}, \qquad (2)$$

где V_{ij} – коэффициент весомости, при определении априорного значения данного параметра учитываются такие параметры, как стаж, ученая степень, сертифицирование международными организациями и другие титулы эксперта; D_{ij} – экспертная достоверность, которая определяется в сравнении с отзывами аналогичных, конкурентных экспертных групп, а также на основе международных стандартов.

Для определения коэффициента весомости существует несколько подходов. Для получения более детальных результатов используется подход, базирующийся на аналитических методах определения коэффициентов весомости [2, 5, 6]. Использование экспертного метода не всегда предоставляет возможность получения детальных результатов.

Выделяя вышеперечисленные априорные показатели безопасности программных комплексов как основу квалиметрических данных, возможно разделить программные комплексы на следующие подкатегории [1, 4]:

Моноструктурные – программный комплекс состоит из программного кода без разделов, цельной архитектуры неблочной структуры, и все операции, связанные с переработкой элементов безопасности, происходят на одном уровне с другими операциями, которые нужны для поддержки функционирования программного комплекса в течение всего жизненного цикла. Данный подход на практике реализуется довольно редко из-за негибкости программного комплекса и нерационального использования вычислительных ресурсов. Основной метод применения программных средств, обладающих внутренней структурой, реализованной с помощью данной тактики, применяется при предотвращении однотипных угроз и атак, где характер и образ угрозы не меняются.

Одноступенчатые – в данной ситуации программный комплекс состоит из программного кода с разделами, цельной архитектуры блочной структуры. Все операции, связанные с переработкой элементов безопасности и другими операциями, которые нужны для поддержки функционирования программного комплекса в течение всего жизненного цикла, реализуются на разных уровнях. Взаимосвязь между уровнями внутренней системы происходит через единый интерфейс, реализованный отдельным блоком программного кода, функционирующим на одном уровне со всеми остальными операциями, которые поддерживают работу программного комплекса в целом. В данной системе особое внимание должно направляться на управление безопасностью самого интерфейса, который играет роль взаимосвязи между двумя внутренними уровнями архитектуры программного комплекса – уровнем переработки элементов безопасности и уровнем, отвечающим за полнофункциональность программного комплекса за весь период жизненного цикла.

Полиструктурные – при таком подходе программный комплекс состоит из программного кода с разделами и нескольких различных, но заранее определенных архитектур блочной структуры. Операции, связанные с переработкой элементов безопасности, одновременно реализуются на различных и нескольких уровнях заранее определенных архитектур программного комплекса. Для сравнительного анализа полученных результатов и принятия решения программным комплексом используется единый интерфейс, функционирующий на основе меняющегося алгоритма, который в свою очередь реализован отдельным независимым модулем в общей архитектуре программного комплекса. Все остальные побочные операции, которые нужны для поддержки функционирования программного комплекса в течение всего жизненного цикла, реализуются на разных уровнях, частичным образом. Реализованные механизмы защиты и алгоритмы также регулярно в течение жизненного цикла программного комплекса верифицируют единый интерфейс принятия решений, так как он сам может подвергнуться атаке. В механизме данного подхода также реализуется алгоритм

обнаружения в программных кодах элементов, разрушающих программные средства. Что в свою очередь решает вопрос безопасности программных средств на более раннем этапе, так как анализу на безопасность подвергается непосредственно исполняемый код программы, а не сервисы, предоставляемые программными средствами. На сегодняшний день в механизме внутренней архитектуры большинства программных комплексов, реализующих систему защиты информации КС, лежит данный подход [7]. Невзирая на тот факт, что для реализации программных комплексов, функционирующих с данной внутренней архитектурой, нужны очень серьезные финансовые затраты, так как расходы на вычислительные системы и аппаратные расходы по сравнению с предыдущими механизмами, перечисленными выше, возрастают в несколько раз, на практике данный подход нашел свое широкое применение.

3. Механизм определения надежности квалиметрических показателей

В арсенале современных систем управлений КС существует целый ряд разнонаправленных и многофункциональных программных комплексов, которые функционируют с постоянной угрозой атаки со стороны злоумышленника, а также во время эксплуатации на практике возникают различные неисправности, что в свою очередь называется отказом. Надежность квалиметрических показателей безопасности программных комплексов – это свойство априорных элементов безопасности сохранять заранее определенные единой политикой безопасности значения качественных характеристик в течение заданного интервала эксплуатационного периода [5, 7]. С точки зрения классической теории надежности надежность метрологических данных элементов безопасности программных комплексов характеризуется интенсивностью отказов, вероятностью безотказной работы и наработкой на отказ.

Если посмотреть на надежность квалиметрических показателей безопасности программных комплексов с классической точки зрения, то интенсивность однотипных отказов возможно сформулировать в следующей форме:

$$\varphi_{моно} = \frac{n(t)}{q_i \Delta_t}, \qquad (3)$$

где $n(t)$ – число однотипных отказов; Δ_t – промежуток времени между однотипными отказами; q_i – количество элементов i-го типа.

Одним из важных аспектов надежности квалиметрических показателей безопасности программных комплексов является вероятность безотказной работы в течение заданного эксплуатационного периода или жизненного цикла программного средства. Вероятность безотказной работы возможно выразить следующим образом:

$$P(t) = \exp(-\int_0^i \varphi_{моно}(t)\,dt). \qquad (4)$$

Не менее важную роль играет характеристика надежности квалиметрических показателей безопасности программных комплексов – наработка на отказ. Характеристику надежности, наработку на отказ возможно сформулировать следующим образом:

$$R = \int_0^{\infty} P(t)\,dt\,. \tag{5}$$

В практике системы управления КС и ее составной части – системы защиты информации, которая состоит из программных комплексов, также встречаются отказы, интенсивность которых не зависит от эксплуатационного времени или от интервала времени с заранее определенной единой политикой безопасности. Такие отказы называются внезапными отказами, и их возможно сформулировать следующим образом:

$$\varphi_{моно}(t) = \varphi_{моно} = const, \tag{6}$$

$$P(t) = \exp(-\varphi_{моно} t), \tag{7}$$

$$R = \frac{K}{\varphi_{моно}}\,, \tag{8}$$

где K – число отказов в течение эксплуатационного периода.

Исходя из данных формул и общей стратегии, возможно также рассчитать интервал, где обеспечивается заданная вероятность безотказной работы системы управления безопасностью программного комплекса, посредством следующей формулы:

$$I_{БР} = \frac{\ln(1 - P_{МО})}{\ln P(t)}\,, \tag{9}$$

где $I_{БР}$ – интервал безотказной работы; $P_{МО}$– вероятность отказа за время между проверками; $P(t)$ – вероятность безотказной работы, определенной единой политикой безопасности.

Заключение

На основе проведенного анализа выявлено преимущество подхода оценки безопасности программных комплексов, составляющих основу систему управления КС, с точки зрения квалиметрических показателей. Так как существование угроз для качества функционирования программных комплексов приводит к пробелам в системе безопасности программных средств и системы управления КС в целом, были изучены основы квалиметрических показателей. Также на основе проанализированных выше подходов измерения качества функционирования систем управления КС предложен механизм определения надежности квалиметрических показателей безопасности программных комплексов.

Литература

1. Rəhimov E.R. Korporativ şəbəkələrin idarə edilməsi. Bakı: İnformasiyaTexnologiyaları, 2008, 322 s.
2. Федюкин В.К. Основы квалиметрии. Управление качеством продукции. М.: Финиль, 2004, 295 с.
3. Круглов В.И., Александровская Л.Н., Аронов И.З., Смирнов В.В. Сертификация сложных технических систем. М.: Логос, 2001, 312 с.

4. Владимирцев А.В., Маругин В.М., Марцынковский О.А., Шеханов Ю.Ф. Применение методов квалиметрической экспертизы в системе менеджмента организации // Науч. труды ВИТУ, вып. 88, СПб.: ВИТУ, 2003, 200 с.
5. Фомин В.Н. Квалиметрия. Управление качеством. Сертификация. Киев: Тандем, 2000, 320 с.
6. Лифиц И.М. Стандартизация, метрология и сертификация. М.: Юрайт, 2007, 399 с.
7. Гусятников В.Н., Безруков А.И. Стандартизация и разработка программных систем. М: Финансы и статистика, 2010, 288 с.

UOT 004.05

Rəhimov Elşən R.
AMEA İnformasiyaTexnologiyaları İnstitutu, Bakı, Azərbaycan.
elshan_rahimoff@mail.ru

Korporativ şəbəkələrin idarəetmə sistemini həyata keçirən proqram təminatı komplekslərinin təhlükəsizliyinin kvalimetrik göstəriciləri.

Məqalə korporativ şəbəkələrin idarəetmə sistemində əsas rol oynayan proqram təminatı komplekslərinin təhlükəsizliyinin kvalimetrik göstəricilərinin təyin olunmasına həsr olunmuşdur. Keyfiyyət xarakteristikalrının təyin olunması vasitəsi ilə proqram təminatı təhlükəsizliyin ilkin elemntlərinin müəyyən olunması göstərilmişdir. Bu yanaşmanın əsasında kvalimetrik verilənlərin etibarlılığını müəyyən edən mexanizm işlənib hazırlanmışdır.

Açar sözlər: *təhlükəsizlik, imtina, informasiya təhlükəsizlik sistemi, proqram təminatı kompleksi, korporativ şəbəkə,kvalimetrik göstəricilər.*

Elshan R. Rahimov
Institute of Information Technology ANAS, Baku, Azerbaijan.
elshan_rahimoff@mail.ru

Qualimetric identificators of security software complexes, which realise corporate network management system.

The paper is dedicated to a question defining of qualimetric identificators of software complexes security which play the main role in corporate network management system. By means of defining quality characteristics the possibility of finding aprior elements of security is shown. On the base of given approach the mecanism of defining of qualimetric data realibility of software complex security was developed.

Key words: *security, failure, information security system, software complex, corporate network, qualimetric identificatiors.*