УДК 004.722.2:621.391

В.Е. Митрохин, П.Г. Рингенблюм

Влияние угроз информационной безопасности на коэффициент готовности телекоммуникационной сети с линейной топологией

Коэффициент готовности – один из важнейших комплексных показателей надежности. Помимо технических факторов, на него также влияют угрозы информационной безопасности. Рассматривается влияние угроз информационной безопасности на коэффициент готовности телекоммуникационной сети.

Ключевые слова: телекоммуникации, информационная безопасность, надежность, коэффициент готовности.

Одним из важнейших комплексных показателей надежности телекоммуникационной сети является ее коэффициент готовности, определяющий вероятность того, что объект окажется в работоспособном состоянии в произвольный момент времени, кроме планируемых периодов, в течение которых применение объекта по назначению не предусматривается [1]. Принято считать, что на коэффициент готовности в случае телекоммуникационной сети оказывают влияние коэффициенты готовности ее узлов (телекоммуникационного оборудования) и ребер (линий связи). В настоящей статье к двум перечисленным выше составляющим добавляется влияние на коэффициент готовности угроз информационной безопасности.

В качестве рассматриваемой модели используется сеть линейной топологии из трех узлов (рис. 1), в которой рассчитывается коэффициент готовности линии связи между узлами *1* и *3*. В качестве линий связи используются сегменты сети Интернет. Угрозы информационной безопасности, вероятности их возникновения и ожидаемый простой системы, связанный с восстановлением работоспособности после реализованной угрозы, определены на основании статистических данных CSI Computer Crime and Security Survey [2]. Статистическая информация обрабатывалась применительно к организациям финансовой сферы экономики Российской Федерации и сети Интернет в качестве среды передачи информации. Для выполнения расчетов топология сети формализована до схемы (рис. 2), в которой в зависимости от состава оборудования в качестве узлов могут выступать:

1. Маршрутизатор Cisco Router.
2. Маршрутизатор Cisco Router и blackbox (виртуальное устройство, отражающее своим коэффициентом готовности влияние угроз информационной безопасности на остальные элементы моделируемой сети).
3. Маршрутизатор Cisco Router и ПАК «ФПСУ-IP».

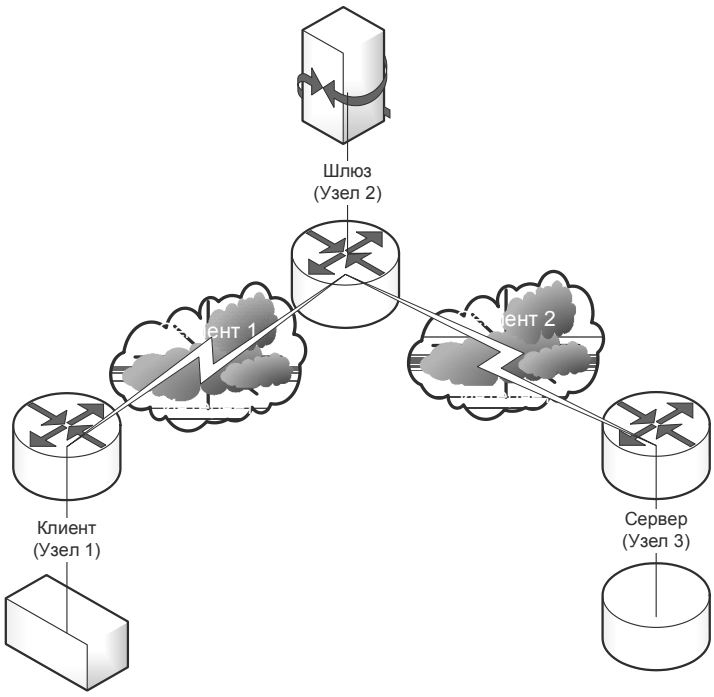

Рис. 1. Моделируемая сеть

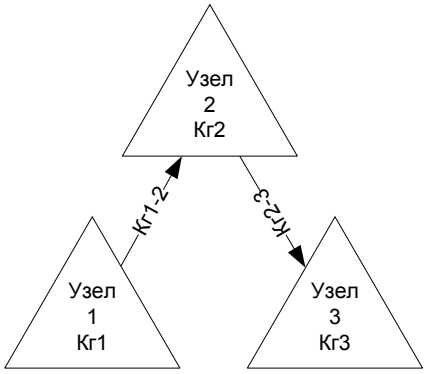

Рис. 2. Формализованная топология моделируемой сети

Create PDF files without this message by purchasing novaPDF printer (http://www.novapdf.com)

Коэффициент готовности линии связи между *1* и *3* узлами моделируемой сети рассчитывается по формуле:

$$K_{г-13} = K_{г1} \times K_{г1-2} \times K_{г2} \times K_{г2-3} \times K_{г3}, \quad (1)$$

где $K_{г1}$, $K_{г2}$, $K_{г3}$ – коэффициенты готовности соответствующих узлов; $Kг_{1-2}$, $Kг_{2-3}$ – коэффициенты готовности линий связи между узлами.

Принимая $K_{г1} = K_{г2} = K_{г3} = K_{г-у}$, а $Kг_{1-2} = Kг_{2-3} = K_{г-I}$, формулу коэффициента готовности формализованной топологии сети можно записать как

$$K_{г-13} = K_{г-у}^{3} \times K_{г-i}^{2}. \quad (2)$$

Коэффициент готовности оборудования на узле сети рассчитывается в с учетом времени на внеплановое техническое обслуживание оборудования (связанное с его отключением) и времени на аварийное восстановление работоспособности:

$$K_{г} = \frac{T_{mtbf}}{T_{mtbf} + (T_{то} + T_{восст})}, \quad (3)$$

где T_{mtbf} – среднее время наработки на отказ; $T_{то}$ – время на техническое обслуживание оборудования; $T_{восст}$ – время на аварийное восстановление работоспособности (ремонт).

В рассматриваемой модели рассматриваются коэффициенты готовности следующих элементов: линии связи, магистрального маршрутизатора, ПАК «ФПСУ-IP» и влияния угроз информационной безопасности. Коэффициенты готовности телекоммуникационного оборудовании определены на основе данных, заявленных производителем (время наработки на отказ) [3, 4], и статистических данных за период 2006–2010 гг. Сбербанка России ОАО (количество отказов и время, затраченное на восстановление работоспособности оборудования).

Коэффициент готовности линии связи между узлами сети $K_{г-i}$ принимается равным $K_{г-i}$=0,999.

Коэффициент готовности маршрутизатора Cisco рассчитывается на основании следующих данных [3]: среднее время наработки на отказ для платформы и интерфейсных карт составляет T_{mtbf-r} = 7 лет = 61320 ч; время на ежегодное техническое обслуживание (необходимо отключении оборудования) $T_{то-r}$ = 4 ч × 7 лет = 28 ч; время на аварийное восстановление работоспособности в случае непредвиденного отказа (по статистическим данным 1–2 раза за срок службы, для моделирования принимается 2 раза) $T_{восст-r}$ = = 16 ч × 2 = 32 ч. По (3) получим:

$$K_{г-r} = \frac{61320}{61320 + (28 + 32)} = 0{,}99902.$$

Коэффициент готовности ПАК «ФПСУ-IP» складывается из следующих данных [4]: среднее время наработки на отказ платформы T_{mtbf-f} = 3 года = 26280 ч; время на аварийное восстановление работоспособности (по статистическим данным 1 раз за срок службы) $T_{восст-f}$ = 8 ч. По (3) получим:

$$K_{г-f} = \frac{26280}{26280 + 8} = 0{,}9997.$$

Влияние угроз информационной безопасности на коэффициент готовности телекоммуникационной сети сводится к появлению на каждом узле сети виртуального элемента blackbox. Коэффициент неготовности элемента blackbox представляет собой произведение вероятности возникновения угрозы информационной безопасности (*P*) на коэффициент неготовности реализованной угрозы ($K_{г-у}$), отсюда получаем коэффициент готовности $K_{г-иб}$:

$$K_{г-иб} = 1 - (1 - K_{г-у}) \times P. \quad (4)$$

Вероятность возникновения угрозы информационной безопасности для финансового учреждения Российской Федерации с активами-нетто более 1 млрд. руб. в течение года составляет *P* = 0,07728 [2, 5]. Для целей моделирования примем время восстановления после реализованной угрозы информационной безопасности $T_{восст}$ = 48 ч. Таким образом, (3, 4):

$$K_{г-у} = \frac{8760}{8760 + 48} = 0{,}99455; \qquad K_{г-иб} = 1 - (1 - 0{,}99455) \times 0{,}07728 = 0{,}99958.$$

Соответственно, для трех описанных выше вариантов оборудования на узлах сети коэффициент готовности будет рассчитываться по следующим формулам:

1. Основное оборудование узлов связи – маршрутизатор, дополнительное оборудование отсутствует, влияние угроз информационной безопасности не рассматривается: $K_{г-у} = K_{г-г}$ (5); подставляя (5) в (2), получаем

$$K_{г1-13} = 0{,}99902^3 \times 0{,}999^2 = 0{,}99507 .$$

2. Основное оборудование узлов связи – маршрутизатор, дополнительное оборудование отсутствует, рассматривается влияние угроз информационной безопасности: $K_{г-у} = K_{г-г} \times K_{г-иб}$ (6); подставляя (6) в (2), получаем

$$K_{г2-13} = 0{,}9986^3 \times 0{,}999^2 = 0{,}99381 .$$

3. Основное оборудование узлов связи – маршрутизатор, дополнительное оборудование – ПАК «ФПСУ-IP», использование данного оборудования приводит к парированию рассматриваемых угроз информационной безопасности: $K_{г-у} = K_{г-г} * K_{г-f}$ (7); подставляя (7) в (2), получаем

$$K_{г3-13} = 0{,}99872^3 \times 0{,}999^2 = 0{,}99417 .$$

Таким образом, использование средств защиты информации (ПАК «ФПСУ-IP»), несмотря на снижение коэффициента готовности формализованной топологии по сравнению с установкой только маршрутизатора на узле связи, дает прирост коэффициента готовности в свете парирования угроз информационной безопасности.

Рассмотрим влияние вероятностных составляющих виртуального элемента blackbox (вероятность возникновения угрозы и время восстановления) на общий коэффициент готовности формализованной топологии телекоммуникационной сети. Для оценки влияния построен график зависимости коэффициента готовности линии связи от изменяющихся величин. Для моделирования влияния указанных выше факторов построим два графика изменения коэффициента готовности формализованной топологии для следующих условий (рис. 3):

1. Изменяется вероятность возникновения угрозы информационной безопасности (P).

2. Изменяется время восстановления после реализованной угрозы информационной безопасности ($T_в$).

Остальные факторы, влияющие на коэффициент готовности формализованной топологии, будем считать стабилизированными.

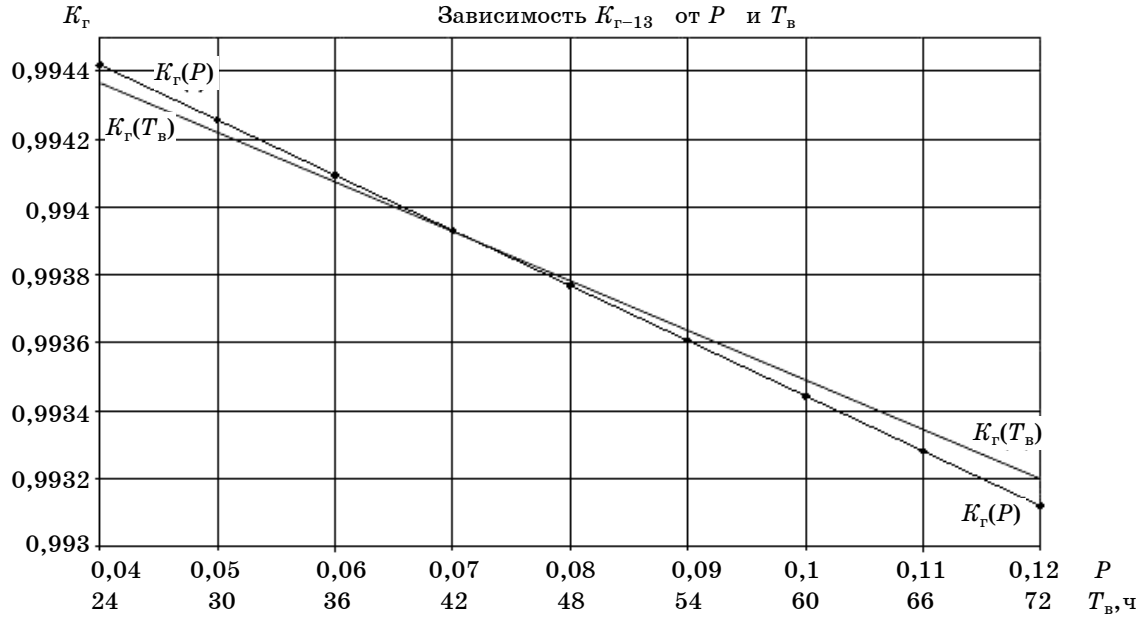

Рис. 3. Зависимость коэффициента готовности сети от вероятности возникновения угрозы информационной безопасности и времени восстановления после реализованной угрозы

Примем диапазоны изменения величин P и $T_в$ размере 50% от расчетного в большую и меньшую стороны. Полученный график свидетельствует о большем влиянии на итоговый коэффициент готовности сети вероятности возникновения угрозы информационной безопасности, нежели времени, затрачиваемого на восстановление работоспособности после реализованной угрозы.

С практической точки зрения, полученные результаты говорят о том, что с точки зрения повышения коэффициента готовности телекоммуникационной сети рационально стремиться минимизировать риски возникновения угроз информационной безопасности, чем добиваться снижения времени, затрачиваемого на восстановление работоспособности сети после инцидента. Помимо описанного в статье повышения коэффициента готовности рассматриваемой телекоммуникационной сети, описанный подход позволяет снизить финансовые и репутационные риски, связанные с инцидентами информационной безопасности.

Литература

1. ГОСТ 27.002-89 Надежность в технике. Основные понятия. Термины и определения. – М.: Стандартинформ, 1990. – 24 с.
2. Richardson R. CSI Computer Crime and Security Survey 2008 / R. Richardson. – CSI, 2009. – 31 p.
3. Одом Ш. Маршрутизаторы CISCO / Ш. Одом, Х. Ноттингем. – М.: Кудиц-Образ, 2003. – 528 с.
4. Руководство администратора ПАК «ФПСУ-IP». – М.: ООО «Фирма «Амикон», 2006. – 18 с.
5. Глобальное исследование утечек. Первое полугодие 2009 [Электронный ресурс]. – Режим доступа: http://infowatch.ru/threats_and_risks/analytical_reports/2811/, свободный (дата обращения: 11.02.2010).

Митрохин Валерий Евгеньевич
Доктор техн. наук,профессор,зав. каф. систем передачи информации Омского государственного университета путей сообщения (ОмГУПС),г. Омск
Тел.: (381-2) 31-06-94
Эл. адрес: mitrokhin@list.ru

Рингенблюм Павел Генрикович
Аспирант каф. системы передачи информации ОмГУПС,г. Омск
Тел.: (381-2) 27-96-71
Эл. адрес: win32conficker@gmail.com

V.E. Mitrokhin, P.G. Ringenbljoum

Influence of threats of informational security on availability of a telecommunication network with linear topology

Availability – one of the major complex metrics of reliability. Besides technical factors it is influenced also by threats of informational security. Influence of threats of informational security on availability of a telecommunication network is considered.
Keywords: telecommunications, information security, reliability, availability.