УДК 004.722.2:621.391

В.Е. Митрохин, П.Г. Рингенблюм

Оценка влияния угроз информационной безопасности на доступность телекоммуникационной сети

Рассматривается оценка влияния угроз информационной безопасности на коэффициент готовности как на один из основных показателей телекоммуникационных сетей с использованием мнимого устройства, включаемого в состав оборудования узлов связи и отражающего влияние угроз информационной безопасности на сеть связи.

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

Под угрозой безопасности информации понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. По цели воздействия на информационную систему угрозы информационной безопасности делятся на угрозы целостности, конфиденциальности и доступности циркулирующей в ней информации.

Успешно реализованная угроза доступности информации в телекоммуникационной сети (ТКС), в отличие от угроз, направленных на другие свойства информации, приводит к простою атакованных информационных служб и как к крайнему варианту всей ТКС. Время простоя элементов ТКС возможно оценить количественно и включить его в расчет коэффициента готовности каждого рассматриваемого элемента как одну из составляющих времени восстановления работоспособности элемента, и далее – всей ТКС, что позволит в дальнейшем оценить ее защищенность от угроз этого типа.

В 2013 г. к широко распространенным фактическим угрозам информационной безопасности добавились хорошо известные исторически, но вследствие крайне малой распространенности не входящие в статистические выкладки и модели угроз, используемые коммерческими предприятиями угрозы доступности информации, связанные с паразитными электромагнитными излучениями и наводками (ПЭМИН). В результате скандальных публикаций Э. Сноуденом выдержек из каталогов программно-аппаратных средств, стоящих на вооружении АНБ США, достоянием общественности стала информация о программно-аппаратных закладках для слежения и деструктивных воздействий на оборудование, устанавливаемое на узлах связи ТКС. Были обнародованы программные и аппаратные закладки, предназначенные для скрытой установки в маршрутизаторы и межсетевые экраны, широко применяемые для построения ТКС, позволяющие производить полностью скрытое удаленное управление скомпрометированными устройствами и зеркалирование передаваемой информации. В силу этого появилась необходимость рассматривать эти угрозы при проектировании и оценке защищенных ТКС. В связи с отсутствием сложившейся практики моделирования угроз информационной безопасности такого рода предлагается использовать нижеследующий метод, хорошо зарекомендовавший себя для моделирования угроз информационной безопасности в сложных и разветвленных ТКС.

Для численной оценки влияния угроз информационной безопасности на доступность телекоммуникационной сети предлагается воспользоваться математическим аппаратом коэффициента готовности как наиболее гибкого и реалистичного стандартизованного показателя надежности. В этих целях введем в состав оборудования, расположенного на узле связи ТКС, мнимое устройство, влияние коэффициента готовности которого будет отражать влияние угроз информационной безопасности на доступность рассматриваемого узла связи.

Коэффициент готовности мнимого устройства ($K_{\text{Г}}^{\text{В}}$) будет складываться из вероятности возникновения соответствующей угрозы информационной безопасности ($P_{\text{В}}$), вероятности ее реализации ($P_{\text{Р}}$) и коэффициента неготовности реализованной угрозы ($K_{\text{НГ}}^{\text{Р.У}}$), отражающего временной интервал, обусловленный простоем узла ТКС, вызванным устранением реализованной угрозы и ее

последствий. Исходя из того, что для оказания влияния на общий коэффициент готовности системы все три события (возникновение угрозы, успешная реализация угрозы, простой в результате реализации угрозы и устранения ее последствий) должны произойти одновременно, то согласно формулам определения полной вероятности коэффициент готовности элемента, отражающего влияние угроз информационной безопасности ($K_{\text{Г}}^{\text{В}}$), определяется следующим образом:

$$K_{Г}^{В} = 1 - K_{НГ}^{Р.У} \times P_{В} \times P_{В} . \quad (1)$$

Коэффициент неготовности реализованной угрозы ($K_{\text{НГ}}^{\text{Р.У}}$) отражает влияние реализованных угроз информационной безопасности на коэффициент готовности элемента телекоммуникационной системы. Тем не менее вероятность возникновения и успешной реализации угрозы информационной безопасности на определенном узле телекоммуникационной системы отлична от 1. Для учета этого фактора необходимо ввести в формулу расчета коэффициента готовности вероятность возникновения и реализации угрозы информационной безопасности.

Вероятность возникновения угрозы информационной безопасности ($P_{\text{В}}$) определяется на основании статистических данных, включающих в себя общую статистику по инцидентам информационной безопасности. Рассмотрим механизм оценки влияния угроз информационной безопасности на примере закладок АНБ. Вероятность возникновения описанной угрозы для коммерческого предприятия примем $P_{\text{В}} = 0{,}00001$. Вероятность принята минимальной в связи с нацеленностью данной угрозы информационной безопасности на стратегический и правительственный сегмент ТКС. Однако полностью исключить эту угрозу коммерческим предприятиям нельзя по причине отсутствия механизмов четкой таргетированности, т.е. возможно срабатывание закладки в оборудовании, изначально предназначенном для установки в критичных объектах сетевой инфраструктуры Российской Федерации, но установленном в коммерческом предприятии.

Вероятность реализации угрозы информационной безопасности ($P_{\text{Р}}$) зависит от применяемого для защиты телекоммуникационного оборудования и определяется на основании модели угроз, разработанной для конкретного узла в топологии сети и определенного оборудования, применяемого на этом узле. Для рассматриваемой в качестве примера угрозы вероятность реализации угрозы $P_{\text{Р}} = 1$ по причине отсутствия на сегодняшний день механизмов превентивной защиты от программно-аппаратных закладок.

Коэффициентом неготовности называется вероятность того, что рассматриваемый объект или система будет находиться в неработоспособном состоянии в период времени, когда предусматривается его или ее использование по назначению. Определить коэффициент неготовности для заданного периода времени можно по следующей формуле:

$$K_{\text{НГ}} = \frac{t_{\text{В}}}{t_{\text{П}}}, \quad (2)$$

где $t_{\text{П}}$ – общая продолжительность периода; $t_{\text{В}}$ – время восстановления работоспособности (простоя).

Для определения коэффициента неготовности реализованной угрозы необходимо задаться временным интервалом и определить время простоя, вызванного реализацией угрозы информационной безопасности и ее последствий на этом временном интервале.

Рассмотрим коэффициент неготовности, связанный с реализованной угрозой информационной безопасности, связанной с программно-аппаратными закладками в оборудовании узла связи ТКС. Примем среднее время восстановления после инцидента $t_{\text{В}} = 72$ ч. Это время обусловлено необходимостью получения с регионального склада поставщика нового оборудования, подготовки его к работе и установки на место инцидента. Для периода в 1 год $t_{\text{П}} = 8760$ ч в соответствии с (2) получаем

$$K_{\text{НГ}} = \frac{72}{87960} = 0{,}0082192 . \quad (3)$$

Исходя из (1) и (3), коэффициент готовности мнимого устройства узла связи, связанного с этой угрозой информационной безопасности, будет составлять

$$K_{\text{Г}} = 1 - (0{,}00001 \times 1 \times 0{,}0082192) = 0{,}9999999 . \quad (4)$$

Аналогично рассчитываются коэффициенты готовности для остальных актуальных угроз информационной безопасности. Результаты расчетов сведены в таблицу.

Вероятности возникновения, реализации и коэффициент неготовности угроз информационной безопасности

№ п/п	Вид угрозы информационной безопасности	$P_В$	$P_Р$	$t_В$	$K_{НГ}^{Р.У}$
1	Атаки типа отказ в обслуживании	0,23667	0,6	4,6	0,00052476
2	Мошенничество в сфере телекоммуникаций	0,06	1	1	0,00011408
3	Вредоносное ПО	0,55667	0,2	24	0,0027379
4	Проникновение в систему извне	0,13667	0,1	2	0,00022816
5	Саботаж	0,03	1	48	0,0054758
6	Инциденты с беспроводными сетями	0,15	1	3,4	0,00038786
7	Ботнеты	0,205	0,4	24	0,0027379
8	Атаки на службу доменных имен	0,07	0,2	1	0,00011408
9	Внедрение закладок на оборудование ТКС	0,00001	1	72	0,0082192

Остальные актуальные угрозы информационной безопасности рассматриваются аналогично и рассчитываются по формулам (1)–(4) на основе данных из таблицы, которые затем последовательно объединяются в единый блок коэффициента готовности угроз информационной безопасности:

$$K_Г^B = K_Г^{У1} \times K_Г^{У1} \times \cdots \times K_Г^{У9}. \quad (5)$$

Подставив в (5) результаты предыдущих вычислений, получим

$$K_Г^B = 0{,}9999255 \times 0{,}9999932 \times 0{,}9999969 \times 0{,}9998357 \times 0{,}9999418 \times 0{,}9997755 \times 0{,}9999984 \times \times 0{,}9999999 = 0{,}9991624. \quad (6)$$

Таким образом, в (6) получено значение коэффициента готовности мнимого устройства, отражающего влияние угроз информационной безопасности, направленных на доступность информации, на надежность ТКС. Для дальнейшей оценки защищенности ТКС от угроз такого рода можно воспользоваться методикой, предложенной в [2] и [4].

Литература

1. ГОСТ 27.002–89. Надежность в технике. Основные понятия. Термины и определения. – М.:Стандартинформ, 1990. – 24 с.

2. Митрохин В.Е. Влияние угроз информационной безопасности на коэффициент готовности телекоммуникационной сети с линейной топологией / В.Е. Митрохин, П.Г. Рингенблюм // Доклады ТУСУРа. – 2010. – № 1 (21), ч. 1. – С. 156–160.

3. Миронова В.Г. Модель нарушителя безопасности конфиденциальной безопасности / В.Г. Миронова, А.А. Шелупанов // Информатика и системы управления. – 2012. – № 1. – С. 28–35.

4. Митрохин В.Е. Использование показателей, связанных с коэффициентом готовности для оценки защищенности телекоммуникационной сети от угроз информационной безопасности / В.Е. Митрохин, П.Г. Рингенблюм // Сб. матер. междунар. науч. конгресса и выставки «Интерэкспо Гео-Сибирь». – 2013. – Т. 5, № 2. – С. 102–106.

5. Сопов М.А. Модели повышения уровня информационной безопасности удостоверяющего центра / М.А. Сопов, А.Ю. Крайнов, А.А. Шелупанов // Доклады ТУСУРа. – 2011. – № 2 (24), ч. 3. – С. 211–216.

6. Жабина А.В. Коэффициент готовности развивающихся телекоммуникационных сетей / А.В. Жабина, Зо Зен Чхор // Матер. межрег. информ. конгресса «МИК-2004». – Омск: ОмГТУ, 2004. – Ч. 3. – С. 137–139.

Митрохин Валерий Евгеньевич
Д-р техн. наук, профессор, зав. каф. инфокоммуникационных системы и информационнй безопасности Омского государственного университета путей сообщения (ОмГУПС)
Тел.: 8 (381-2) 31-06-94
Эл. почта: mitrokhin@list.ru

Рингенблюм Павел Генрикович
Аспирант каф. инфокоммуникационных системы и информационной безопасности ОмГУПС
Эл. почта: win32conficker@gmail.com

Mitrokhin V.E., Ringenbljoum P.G.
Assessing the influence of information security threats to the availability of telecommunications network

The estimation of the influence of security threats on the availability factor, as one of the main indicators of telecommunication networks using imaginary device, included to the equipment of communication nodes, is reflecting the impact of security threats on the communication networks.
Keywords: telecommunications, information security, reliability, availability.