УДК621.391

# Математическая модель влияния средств защиты информации на характеристики узла связи телекоммуникационной сети

В. Е. Митрохин, П. Г. Рингенблюм

В работе рассматривается подход к созданию математической модели состояний узла связи телекоммуникационной сети в условиях управляющего воздействия технических отказов оборудования узла связи и угроз информационной безопасности. Также в работе дается оценка влияния средств защиты информации на технические характеристики и показатели надежности узла связи телекоммуникационной сети.

*Ключевые слова:* телекоммуникационная сеть, узел связи, средства защиты информации, информационная безопасность, математическая модель, коэффициент готовности.

## 1. Математическая модель работоспособности узла связи телекоммуникационной сети

Работоспособность узла связи телекоммуникационной сети (ТКС) зависит от его способности противостоять влиянию технических отказов оборудования и угроз информационной безопасности (ИБ). События, обуславливающие это влияние, могут привести к переходу узла связи из работоспособного состояния в неработоспособное. Процесс воздействия этих событий на узел связи ТКС не является детерминированным по своим параметрам, и управляющими в этом процессе являются потоки соответствующих отказов. По своей природе и в соответствии с [1] потоки всех рассматриваемых отказов характеризуются экспоненциальным законом распределения. Экспоненциальный характер потоков событий, управляющих состояниями узла связи ТКС, позволяет использовать аппарат марковских случайных процессов с непрерывным временем и дискретными состояниями. Такими состояниями будут являться:

1. Узел связи ТКС находится в состоянии готовности.
2. Узел связи ТКС находится в состоянии неготовности по причине технического отказа оборудования.
3. Узел связи ТКС находится в состоянии неготовности по причине реализации угрозы ИБ, направленной на нарушение доступности информации.

Таким образом, состояние узла связи можно представить в виде графа (рис. 1). В рамках своей природы исследуемые процессы являются установившимися, то есть временем перехода из состояния в состояние можно пренебречь, следовательно узел связи ТКС весь рассматриваемый период времени находится только в одном из трех описанных выше состояний, что описывается формулой:

$$P_1(t) + P_2(t) + P_3(t) = 1,$$

где $P_1(t)$, $P_1(t)$, $P_1(t)$ – вероятности нахождения узла связи в соответствующих состояниях.

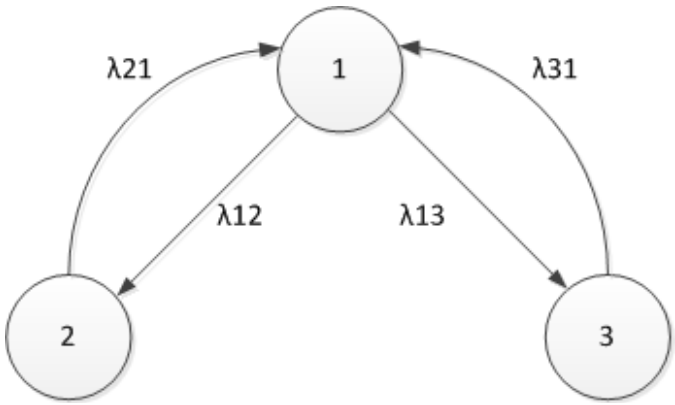


Рис. 1. Граф состояний узла связи ТКС

Поскольку физическим смыслом коэффициента готовности (Кг) и коэффициента неготовности (Кнг) является вероятность нахождения элемента соответственно в работоспособном и неработоспособном состоянии, то можно записать:

$$Кг + Кнг_o + Кнг_y = 1,$$

где $Кг$ – Кг узла связи ТКС; $Кнг_o$ – Кнг, обусловленный техническими отказами оборудования узла связи ТКС; $Кнг_y$ – Кнг, обусловленный влиянием угроз ИБ.

В соответствии с [2] $Кнг_o$ определяется по следующей формуле:

$$Кнг_o = 1 - \frac{1}{t_2 - t_1}\int_{t_1}^{t_2} e^{-\lambda_{12}t}dt,$$

где $t_1$, $t_2$ – моменты времени начала и конца исследуемого интервала; $\lambda_{12}$ – параметр интенсивности потока отказов.

Методика расчета $Кнг_o$ хорошо изучена и описана в научных публикациях и рекомендациях для инженерных расчетов [3]. В то же время единой общепринятой методики расчета $Кнг_y$ не существует. В настоящей работе предлагается рассматривать механизм воздействия угроз ИБ, направленных на нарушение доступности информации, по аналогии с техническими отказами оборудования узла связи, поскольку конечным результатом воздействия угроз ИБ этого типа является переход узла связи ТКС из работоспособного состояния в неработоспособное, что так же, как и технические отказы оборудования узла связи ТКС, входит в расчет величины Кг. В [4] предлагается рассчитывать $Кнг_y$ по следующей формуле:

$$Кнг_y = P_B \times P_P \times Кнг^{РУ},$$

где $P_B$ – вероятность возникновения угрозы ИБ на исследуемом узле связи ТКС; $P_P$ – вероятность реализации угрозы ИБ на исследуемом узле связи ТКС; $Кнг^{РУ}$ – *Кнг*, обусловленный временем простоя узла связи по причине реализации угрозы ИБ, рассчитанный в предположении, что на исследуемом узле связи угроза ИБ возникла и была реализована. Методы оценки угроз ИБ достаточно подробно рассмотрены в работах [5–9].

Исходя из природы и физического смысла величины $Кнг_y$, все мероприятия в рамках обеспечение ИБ ТКС должны быть направлены на снижение значения $Кнг_y$. Поскольку каждая из составляющих ее трех величин не зависит от остальных, зависимость $Кнг_y$ от величин его составляющих при двух стабилизированных показателях из трех является линейной. Скорость изменения любой функции характеризуется ее производной. В случае линейной функции ее частной производной является коэффициент перед аргументом, таким образом, скорость возрастания будет характеризоваться произведением стабилизированных показателей. Следовательно, для уменьшения величины $Кнг_y$ необходимо воздействовать на ту ее

составляющую, значение которой наибольшее. Путем анализа физического смысла и возможности влияния на эти величины определено нижеследующее.

$Кнг^{РУ}$ определяется временем нахождения узла связи ТКС в состоянии неготовности. Это время может складываться из времени нахождения узла связи в атакуемом состоянии, временного интервала, необходимого для активизации средств защиты информации (СЗИ), предназначенных для борьбы с соответствующими угрозами ИБ или активизации решения для аутсорсинга защиты от атак типа «отказ в обслуживании» (DoS). Таким образом, у атакуемой ТКС возможность воздействовать на время нахождения узла связи в неработоспособном состоянии отсутствует. В случае успешной реализации атаки это время будет определяться только возможностями злоумышленника.

$P_B$ угрозы ИБ, направленной против узла ТКС, зависит только от привлекательности цели для злоумышленников. В случае крупной организации значение $P_B$ стремится к 1. По данным компаний, специализирующихся на аналитике в области ИБ, все крупнейшие организации Российской Федерации подвергаются регулярным атакам, направленным на нарушение доступности сетевых служб. Таким образом, принимая тот факт, что исследуемая ТКС достоверно будет подвергаться атакам злоумышленников, при условии одинаковой привлекательности всех узлов связи ТКС для атак, $P_B$ угрозы ИБ для исследуемого узла ТКС будет зависеть от общего числа узлов сети, доступных атакующим, и общего числа атак за рассматриваемый период. Таким образом, возможность влиять на значение $P_B$ со стороны исследуемой ТКС отсутствует.

$P_P$ угрозы ИБ, направленной против узла ТКС, защищаемого при помощи СЗИ, установленных непосредственно на узле связи, будет зависеть в первую очередь от совершенства защитных механизмов СЗИ. Таким образом, $P_P$ является единственным доступным показателем для воздействия на величину $Кнг_у$ со стороны ТКС.

Воздействовать на величину $P_P$ возможно при помощи включения в состав оборудования узла связи ТКС специализированных СЗИ, предназначенных для защиты от угроз ИБ, направленных на нарушение доступности информации. Однако как любое техническое устройство, СЗИ несовершенны и оказывают влияние не только на защищенность узла связи от угроз ИБ, но и на технические характеристики узла связи и его показатели надежности. Одним из таких СЗИ, широко применяемых для защиты корпоративных сетей передачи данных, является ПАК «ФПСУ-IP» производства ООО «Амикон» (Российская Федерация). Защита от угроз ИБ, направленных на нарушение доступности информации, не является основным предназначением этих СЗИ [5], но тем не менее их применимость для этой цели рассмотрена далее и подтверждена экспериментально. Как любое техническое устройство, ПАК «ФПСУ-IP» подвержен техническим отказам и, соответственно, оказывает влияние на $Кнг_о$ узла связи. Механизм этого влияния описан в [6] и полностью аналогичен влиянию любого другого устройства из состава оборудования узла связи. Также ПАК «ФПСУ-IP» может оказывать негативное влияние на такие характеристики сегмента ТКС, как время отклика удаленного ресурса и пропускная способность сегмента ТКС. Оценка этого влияния выполнена в [7], и несмотря на незначительные ухудшения характеристик сегмента ТКС, применение ПАК «ФПСУ-IP» не оказывает видимого негативного влияния на производительность корпоративных информационных систем. Представленная модель не включает в себя учет влияния угроз ИБ, направленных на линии связи (ребра сети). Кг ребер сети является известным, а его значения – нормируемыми.

## 2. Имитационное моделирование сегмента ТКС в условиях атаки типа «отказ в обслуживании»

$P_P$ угрозы ИБ следует рассматривать в зависимости от используемого на узле связи оборудования и СЗИ. Рассмотрим влияние СЗИ на $P_P$ угрозы ИБ на примере ПАК «ФПСУ-IP». Подсистема фильтрации СЗИ ПАК «ФПСУ-IP» позволяет значительно снизить вероятность успешной реализации атаки типа DoS, блокируя атакующий трафик на уровне СЗИ и не пропуская его к оборудованию, уязвимому для атак этого вида. Тем не менее с установленным ПАК «ФПСУ-IP» узел связи остается уязвимым к атакам, направленным на полную утилизацию канала связи. Как отмечено в [8, 9], доля атак такого типа в связи со значительным ростом пропускной способности каналов снижается, и актуальными на сегодняшний день остаются атаки, направленные на утилизацию вычислительной мощности оборудования, противодействие которым осуществимо при помощи ПАК «ФПСУ-IP» и аналогичных СЗИ. Таким образом, $P_P$ зависит исключительно от состава оборудования на узле связи ТКС и применяемых в этом оборудовании защитных механизмов.

Для оценки влияния СЗИ на $P_P$ проведена серия экспериментов, позволяющих оценить применимость ПАК «ФПСУ-IP» для защиты узлов ТКС от атак типа (DoS). В ходе экспериментов проведено имитационное моделирование атаки типа DoS на узел ТКС одновременно с замером времени отклика и пропускной способности канала связи. Моделирование произведено на стенде, собранном в соответствии с рис. 2.

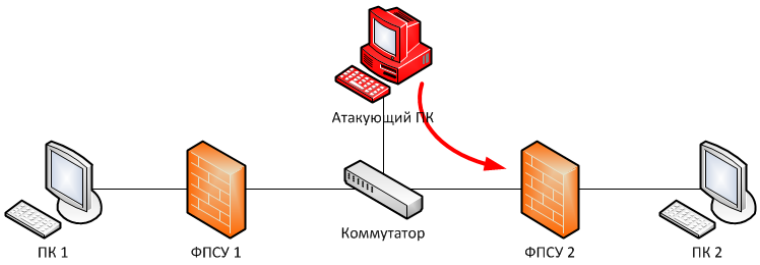


Рис. 2. Схема модели сегмента ТКС для определения времени отклика и пропускной способности сегментаТКС

Проведены 4 эксперимента со следующими условиями:

1. В составе оборудования моделируемого сегмента ТКС отсутствуют СЗИ ПАК «ФПСУ-IP», имитация атаки типа DoS не производится (эталонное измерение).
2. В составе оборудования моделируемого сегмента ТКС присутствуют СЗИ ПАК «ФПСУ-IP», имитация атаки типа DoS не производится (оценка влияния СЗИ на характеристики сегмента ТКС).
3. В составе оборудования моделируемого сегмента ТКС отсутствуют СЗИ ПАК «ФПСУ-IP», производится имитация атаки типа DoS (контрольное измерение, демонстрирующее неспособность сегмента ТКС выполнять функции передачи данных в условиях атаки типа DoS).
4. В составе оборудования моделируемого сегмента ТКС присутствуют СЗИ ПАК «ФПСУ-IP», производится имитация атаки типа DoS (оценка способности СЗИ противостоять атакам типа DoS).

Для проведения моделирования использовано следующее программное и аппаратное обеспечение:

1. ПК1 и ПК2 – персональный компьютер HP DC7700SFF CPU Intel Core 2 Duo 2.13 GHz, 2 GB RAM, LAN Intel PRO1000CT, ОС Windows 7 Professional RUS x86.
2. Атакующий ПК – персональный компьютер HP DC7700SFF CPU Intel Core 2 Duo 2.13 GHz, 2 GB RAM, LAN Intel PRO1000CT, ОС Debian Linux 7.

3. ФПСУ 1 и ФПСУ 2 – СЗИ ПАК «ФПСУ-IP» 2013 г.в. сверхвысокой производительности (производства ООО «Амикон», Российская Федерация).
4. Коммутатор H3C S5500 (коммутатор уровня ядра сети с производительностью коммутирующей матрицы 128 гигабит в секунду / 95000000 пакетов в секунду).

Измерение характеристик сегмента ТКС произведено по нижеследующей методике. Для оценки задержек при прохождении информационного трафика через телекоммуникационное оборудование используется программное обеспечение (ПО) «HRPing v5.06» (бесплатное ПО разработки cFos Software GmbH), для оценки пиковой пропускной способности стенда используется ПО «IPerf measurment tool v.2.0.5-2» разработки University of Illinois.

ПО HRPing производит высокоточное измерение времени отклика путем отправки запроса входящего эха по протоколу ICMP и измерения времени между отправкой запроса и получением ответа. Протокол ICMP входит в стек протоколов TCP/IP и используется для передачи сервисной информации. Предел точности измерений ПО HRPing составляет 1 мкс. ПО IPerf является клиент-серверной утилитой для тестирования пропускной способности сети. Предел точности измерений ПО IPerf составляет 1 кбит/с. Обе программы являются свободно распространяемыми.

Моделирование атаки типа «отказ в обслуживании» произведено следующим образом: персональные компьютеры (ПК) и СЗИ ПАК «ФПСУ-IP» объединены в локальную сеть при помощи высокопроизводительного коммутатора второго уровня H3C S5500 Series в соответствии со схемой (рис. 2). Коммутационная матрица используемого коммутатора обеспечивает уровень быстродействия, эквивалентный прямому сетевому подключению на рассматриваемых значениях сетевой нагрузки. Также в коммутатор включен атакующий ПК. На атакующем ПК под управлением ОС Debian Linux на базе свободного программного обеспечения «pktgen v2.7.7» развернут комплекс, имитирующий атаку типа DoS. Данное ПО производит рассылку пакетов, направленную на полную утилизацию канала связи, производительности сетевого интерфейса и вычислительных мощностей атакуемого узла.

После запуска ПО, имитирующего атаку, производится замер времени отклика и пиковой пропускной способности канала связи. Также при измерении времени отклика производится оценка числа потерянных пакетов (запросы, ответы на которые не были получены в отведенное для этого время). Таким образом, определено среднее время прохождение пакета с одного ПК на другой в направлении атакуемого ПК и процент потерянных пакетов. Определение пиковой пропускной способности произведено встроенными средствами программного обеспечения IPerf Measurement Tool. Эти показатели характеризуют способность сети выполнять свои задачи в условиях атаки типа DoS. Результаты всех измерений сведены в табл. 1.

Таблица 1. Производительность моделируемого сегмента ТКС

| № п/п | Измерение | Время отклика, мс | Потеря пакетов, % | Пропускная способность, кбит/с (%) |
|---|---|---|---|---|
| 1 | Без атаки, без СЗИ | 0.160 | 0 | 928653 (100 %) |
| 2 | Без атаки, ПАК «ФПСУ-IP» | 0.396 | 0 | 893101 (96 %) |
| 3 | DoS-атака, без СЗИ | 0.163 | 29 | 306116 (33 %) |
| 4 | DoS-атака, ПАК «ФПСУ-IP» | 8.966 | 0 | 467688 (50 %) |

Таким образом, падение пиковой пропускной способности моделируемого сегмента ТКС составило более 65 % (измерение 3) по сравнению с эталонным значением (измерение 1). Время отклика по сравнению с измерением 1 увеличилось незначительно, однако выявленный процент потери пакетов фактически приводит к невозможности сетевого сегмента выполнять функции по передаче данных. Таким образом, в рамках рассматриваемой модели атака типа DoS, направленная на моделируемый узел связи, приводит к его неработоспособности.

Аналогичным образом произведено моделирование атаки типа DoS с использованием на узле связи СЗИ (измерение 4). ПАК «ФПСУ-IP» объединены в сеть с использованием коммутатора. Информационный обмен межу ПК 1 и ПК 2 осуществляется через туннель виртуальной частной сети, формируемый ПАК «ФПСУ-IP». Несмотря на возросшее время отклика и снизившуюся пропускную способность, работоспособность моделируемого сегмента ТКС сохранилась, что позволяет ТКС выполнять свои функции. Таким образом, по результатам проведенных экспериментов можно сделать следующие выводы о влиянии атаки типа DoS на функционирование узла ТКС:

1. При атаке на узел связи моделируемого сегмента без применения СЗИ число потерянных пакетов не позволяет обеспечить нормальное функционирование услуг связи.
2. При использовании в качестве СЗИ ПАК «ФПСУ-IP» возрастает среднее время отклика атакуемого узла, что связано с задержками в обработке трафика ПАК «ФПСУ-IP» в условии атаки, однако зафиксированный рост времени отклика при отсутствии потерь пакетов не оказывает существенного воздействия на функционирование услуг связи.
3. В условиях атаки типа «отказ в обслуживании» пропускная способность сегмента ТКС значительно снижается, что обуславливается самой природой атаки, однако применение СЗИ на узле связи (в частности, ПАК «ФПСУ-IP») позволяет обеспечить бесперебойное функционирование сегмента ТКС со сниженными, но допустимыми характеристиками.

Результаты эксперимента показали, что применение ПАК «ФПСУ-IP» позволяет обеспечить бесперебойное функционирование сегмента ТКС в условиях продолжительной атаки типа DoS с характеристиками, допустимыми для функционирования сегмента ТКС и осуществления необходимых бизнес-процессов. На основании результатов проведенного моделирования определены значения $P_P$, которые целесообразно применять для построения математической модели. В случае, когда на узле связи ТКС установлен только маршрутизатор (отсутствуют СЗИ), при моделировании атаки типа «отказ в обслуживании» сетевой трафик через моделируемый сегмент не проходит и атакуемый узел находится в состоянии неготовности. Таким образом, при отсутствии на атакуемом узле СЗИ $P_P = 1$. В случае, когда на узле связи ТКС установлено СЗИ ПАК «ФПСУ-IP», применяемое в ПАО Сбербанк для обеспечения конфиденциальности информации, узел связи находится в состоянии готовности, однако он функционирует со сниженными характеристиками. Это отражено в значении $P_P = 0.1$.

## 3. Выводы

1. Математическая модель работоспособности узла связи ТКС как системы из трех состояний полностью применима для описания его состояния с учетом влияния технических отказов оборудования и угроз ИБ.
2. СЗИ оказывает следующее влияние на характеристики узла связи ТКС: повышают $Кнг_o$ за счет технического несовершенства; снижают $Кнг_y$ за счет уменьшения времени простоя, вызванного реализацией угроз ИБ, направленных на нарушение доступности информации; ухудшают технические характеристики сегмента ТКС за счет увеличения времени отклика и снижения пиковой скорости передачи данных.
3. Применение СЗИ для защиты ТКС от угроз ИБ, направленных на нарушение доступности, полностью оправдано, поскольку увеличение Кг за счет снижения времени нахождения узла связи в состоянии неготовности по причине реализации угроз ИБ превосходит его снижения за счет технических отказов СЗИ.
4. Для проведения инженерных расчетов на основе разработанной математической модели обосновано использование величины $P_P = 1$ в случае отсутствия на моделируемом узле связи СЗИ и $P_P = 0.1$ в случае их наличия.

## Литература:


1. *Шелухин О. И.* Моделирование информационных систем. М. : Горячая линия – Телеком, 2012. 516 с.
2. ГОСТ Р 27.002-2009 Надежность в технике. Термины и определения. М: Изд-во ФГУП «СТАНДАРТИНФОРМ», 2011. 28 с.
3. *Зеленский А. В.* Надежность сложных электронных систем специальногоназначения [Электронный ресурс]: электрон. учеб. пособие / А. В. Зеленский, В. А. Зеленский; Минобрнауки России. Самар. гос. аэрокосм. ун-т им. С.П.Королева (нац. исслед. ун-т). Электрон. текстовые и граф. дан. (690Кбайт). Самара 2012. Режим доступа: http://www.ssau.ru/files/education/uch_posob/Надежность%20сложных-Зеленский%20AB.pdf
4. *Митрохин В. Е., Рингенблюм П. Г.* Оценка влияния угроз информационной безопасности на доступность телекоммуникационной сети // Доклады Томского государственного университета систем управления и радиоэлектроники. 2014. № 2 (32). С. 121–124.
5. *Белкин С. А., Белов В. М.* Сравнительный анализ методов оценки угроз информационной безопасности // Доклады V1 Пленума СибРОУМО по образованию в области информационной безопасности и XV конференции, Томск – Иркутск, 9-13 июня 2014 г. Томск: В-Спектр, 2014. С. 188–194.
6. *Плетнев П. В., Белов В. М.* Сравнительный анализ существующих методов определения рисков информационной безопасности // Ползуновский вестник. 2011. №3/1. С. 221–223.
7. *Белкин С. А., Белов В. М., Пивкин Е. Н.* Об общей схеме оценки рисков информационной безопасности // Измерение, контроль, информатизация: материалы XV Международ. науч.-практ. конф. Барнаул: изд-во АлГТУ, 2014. С. 270–272.
8. *Белкин С. А., Белов В. М., Пивкин Е. Н.* Применение факторного планирования эксперимента для оценки вероятностей угроз информационной безопасности // Ползуновский вестник. 2014. № 2. С. 232–234.
9. *Белкин С. А., Белов В. М.* Оценка вероятности угрозы заражения компьютерным вирусом на основе факторного планирования эксперимента // Информационное противодействие угрозам терроризма. 2014. № 23. С. 55–61.
10. Программно-аппаратный комплекс «ФПСУ-IP». Описание применения [Электронный ресурс]. URL: https://amicon.ru/download/fpsu-ip_description.pdf. (дата обращения: 20.01.2016).
11. *Митрохин В. Е., Рингенблюм П. Г.* Влияние угроз информационной безопасности на коэффициент готовности телекоммуникационной сети с линейной топологией // Доклады Томского государственного университета систем управления и радиоэлектроники. 2010. № 1 (21). С. 156–159.
12. *Митрохин В. Е., Рингенблюм П. Г.* Оценка влияния средств защиты информации на характеристики телекоммуникационной сети // Наука, образование и инновации: сборник статей международной научно-практической конференции (28 декабря 2015 г., г. Челябинск), ч. 3. Уфа: РИО МЦИИ ОМЕГА САЙНС, 2015. С. 107–110.
13. Лаборатория Касперского. DDoS атаки в третьем квартале 2015 года [Электронный ресурс]. URL: https://cdn.securelist.ru/files/2015/11/Q3_DDoS_report_RUS.pdf. (дата обращения: 20.01.2016).
14. Лаборатория Касперского.DDoS-атаки во втором квартале 2015 года [Электронный ресурс]. URL:https://securelist.ru/analysis/malware-quarterly/26463/ddos-ataki-vo-vtorom-kvartale-2015-goda/ (дата обращения: 20.01.2016).

**Митрохин Валерий Евгеньевич**
д.т.н., профессор, заведующий кафедрой «Инфокоммуникационные системы и информационная безопасность» ФГБОУ ВО «ОмГУПС», тел. (3812) 31-06-94,
e-mail: mitrokhin@list.ru.

**Рингенблюм Павел Генрикович**
аспирант кафедры «Инфокоммуникационные системы и информационная безопасность» ФГБОУ ВО «ОмГУПС», тел. (3812) 31-06-94, e-mail: win32conficker@gmail.com.

**Mathematical model of the effect of information security facilities on telecommunication center characteristics**

**P. Ringenblyum, V. Mitrokhin**

This article considers an approach to the creation of a mathematical model of telecommunication center states in conditions of managing influence of technical equipment failures of telecommunication centers and information security threats. It also assesses the effect of information security facilities on technical specifications and reliability of telecommunication centers.

*Keywords:* telecommunication network, centers, security appliances, information security, mathematical model, availability.