

# АКТУАЛЬНЫЕ ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ (СЕТЕЙ) ОБЩЕГО ПОЛЬЗОВАНИЯ

**В.О. Шварцман**

Главный технический эксперт ЦНИИС, д.т.н.

## КОЛИЧЕСТВЕННЫЕ ОЦЕНКИ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Одна из принципиальнейших проблем теории и практики обеспечения информационной безопасности (ИБ) систем и сетей связи – отсутствие количественной оценки ее состояния.

О необходимости и важности наличия критерия ИБ свидетельствует тот факт, что ИК-17 МСЭ в октябре 2005 г. учредила специализированную группу "Базовый уровень информационной безопасности сетевых операторов". Целью работы этой группы является определение базового уровня, относительно которого операторы смогут оценивать состояние сетевой и информационной безопасности.

Великий физик У. Томсон (Лорд Кельвин) так охарактеризовал подобную ситуацию: "Если вы можете измерять и выражать в числах то, о чем говорите, то об этом предмете вы кое-что знаете; если же вы не можете сделать этого, то ваши знания скудны и неудовлетворительны" ("Connect" 2, 2002 г.). Убийственная характеристика. И, наверное, в принципе правильная, так как отсутствие меры безопасности создает неопределенность в понимании того, в каком состоянии находится ИБ систем (сетей) связи, какова эффективность методов и средств защиты в отношении повышения ИБ, как соотносятся затраты на защиту с рисками, возникающими при ее отсутствии или недостаточности.

Следует иметь в виду два обстоятельства, смягчающих суровую оценку отсутствия количественной меры ИБ.

Во-первых, ИБ не единственная область использования понятия безопасности, где при всем желании иметь ее количественную оценку она отсутствует. И во многих других областях, если не во всех, количественная оценка безопасности тоже отсутствует. Такой оценки нет и в случае, если речь идет об обеспечении пожарной безопасности, безопасности на производстве, транспорте, в медицине, космонавтике и т.д. и т.п.

Во-вторых, по-видимому не случайно, что отсутствует возможность обеспечения полной, стопроцентной безопасности. Остряки по этому поводу определяют три условия полной ИБ системы:

- ее следует отсоединить от сети связи;
- ее следует поместить в стальной саркофаг;
- саркофаг следует разместить в скалистых горах, где хранится золотой запас США.

Очевидно, что в отношении ИБ систем (сетей) связи эти условия принципиально невыполнимы. Заметим также, что недостаточно определить количественную меру ИБ, надо, еще ответить на другой не менее сложный вопрос: как нормализовать эту меру.

Таким образом, необходимо принять все меры и сосредоточить усилия на все более эффективных методах и средствах защиты и оснащать ими системы (сети) связи. Ведь очевидно, что чем совершеннее организована защита, тем состояние ИБ лучше. Необходимо постараться установить количественную зависимость между объемами использования более совершенных методов и средств защиты и объемами затрат на их создание. В результате получения такой зависимости для различных последствий "прорыва" защиты можно будет выбрать некоторый "квазиоптимальный" ее уровень.

Существует мнение, что причиной отсутствия этой меры является наличие в системах (сетях) связи программного компонента, реализующего протоколы функционирования, ко-

торые делают практически невозможным точное прогнозирование поведения системы (сети) во всех возможных ситуациях.

В настоящее время для оценки ИБ используют несколько методов:

- анализ данных по ИБ реальных систем (сетей) связи;
- натурное экспериментирование;
- имитационное моделирование;
- экспертные оценки.

Все эти методы отличаются большой сложностью реализации и не позволяют получить конкретные и надежные критерии оценки ИБ.

В стандарте отрасли "Системы обеспечения ИБ ВСС РФ. Термины и определения", Минсвязи России ОСТ 45.127 – 99 (введен 01.01.2000) указано, что качественные характеристики работы ССОП – это совокупность параметров, определение, измерение и регулирование которых позволяет достигнуть заданного уровня качества службы ССОП. Между тем формулировка "заданного уровня качества службы" не конкретна, так как в ней отсутствует указание, какие показатели характеризуют этот уровень.

В настоящее время используют четыре основных показателя, характеризующих состояние ИБ:

- вероятность сохранения конфиденциальности охраняемых сведений;
- вероятность нарушения целостности охраняемой информации;
- вероятность блокирования информации и системы управления связью;
- вероятность сохранения целостности сети связи.

Существует специальное математическое обеспечение, так называемый комплекс информационной безопасности (МАКОИБ) АРМ "АРМ-ОБС", который учитывает три первых показателя.

Так как безопасность является одной из характеристик качества услуг, естественно говорить о совокупности параметров, определение, измерение и регулирования которых определяет качество услуг службы (сети) общественного пользования ОП. К сожалению, об этих параметрах в МАКОИБ ничего конкретного не сказано. Это относится не только к безопасности. В таком же положении находятся и параметры качества некоторых услуг, для которых не определены не только вопросы измерения и регулирования, но и сами параметры (характеристики) качества услуг.

Может быть к этому вопросу можно подойти так: "Заданный уровень безопасности" – это такое состояние, когда в условиях несанкционированных действий (НСД) основные характеристики системы связи (достоверность, время передачи определенного объема информации по заданному адресу, доступность, надежность) не ухудшаются. Иными словами, когда меры защиты от угроз ИБ обеспечивают функционирование системы связи в штатном режиме.

В ряде работ предлагается использовать в качестве нормы "базовый уровень информационной безопасности". Он определяется как "разумно достаточный уровень безопасности, обеспечивающий, исходя из критерия эффективности/стоимости, приемлемый для владельцев информации уровень финансовых рисков ее утери, нарушения ее целостности и доступности, а в необходимых случаях и конфиденциальности". Достоинством введения "базового уровня" является единый подход к ИБ и его единство для всех требований. В то же время такой подход имеет много недостатков:

• отсутствуют серьезные обоснования единых значений рекомендуемых требований, поскольку понятие "разумно достаточный" весьма неопределенно;

• положенный в основу "базового уровня" минимальный объем угроз не стимулирует применения наиболее совершенных и, естественно, более дорогих систем защиты;

• принятие "базового уровня" приведет к тому, что реальное положение дел в отношении степени ИБ останется по-прежнему весьма неопределенным;

• использование "базового уровня" не сочетается с методикой обеспечения "принципа минимального риска", принятого МСЭ в рекомендации X.805.

И кроме того, при таком подходе не учитывается рекомендация МСЭ X.805, предусматривающая использование трех уровней безопасности:

• уровень безопасности инфраструктуры, который включает в свой состав устройства передачи информации (маршрутизаторы, коммутаторы, серверы), а также линии связи между ними;

• уровень безопасности сервисов, описывающий принципы защиты услуг, которые предлагает клиентам сервис-провайдер, например доступ в Интернет, сервис freephone, QoS, VPN и т.п.;

• уровень безопасности приложений, определяющий защищенность приложений, предоставляемых клиентам сервис-провайдерами, провайдерами приложений или операторами связи (FTP, web-сервисы, IP-телефония, электронная почта, приложения электронной коммерции и т.п.). На этом уровне рассматривается обеспечение защищенности четырех целей атак: пользователя приложения, провайдера приложения, интегратора и сервис-провайдера.

Остается неясным, к какому или к каким из этих уровней предполагается применять понятие "базового уровня"? И, главное, это понятие неконкретно, так как не известно, как количественно его оценивать.

Существуют несколько методик оценки как отдельных угроз, так и суммарного их воздействия. В принципе эти методики сводятся к следующему:

• проводится оценка воздействия на каждый подвергающийся угрозе объект ("I");

• определяется уровень вероятности воздействия каждой угрозы ("O");

• составляется список степени угроз, ранжированный по коэффициенту подверженности. Используются три возможные значения степени угрозы – высокая (3), средняя (2), низкая (1);

• вся информация представляется в виде таблицы величин угроз.

Пример оценки величины трех видов угроз дан в табл. 1.

Получаемая при этом количественная характеристика суммарного воздействия всех угроз носит не абсолютный, а сравнительный характер. Применение такой методики требует высокой квалификации экспертов, а также использования или разработки специального математического аппарата. Как видно, приведенная методика оценки ИБ в значительной степени субъективна.

В 1990 г. компания C&A Systems Security Ltd. разработала методику и соответствующий инструмент для анализа и управления информационными рисками под названием COBRA. Здесь под риском ИБ системы связи ОП понимается значение вероятности и величина (характер) возможного ущерба пользователя, оператора услуг связи или государства,

Таблица 1

Угрозы	Величина воздействия ("I")	Уровень вероятности воздействия ("O")	Коэффициент подверженности ("I" x "O")	Степень угрозы
A	2	2	4	Средняя (2)
B	1	1	1	Низкая (1)
B	3	2	6	Высокая (3)

полученного вследствие реализации нарушителем угрозы ИБ системы (сети) ОП.

Отметим, что понятие риск отсутствует в ряде правительственных документов по ИБ систем (сетей) связи, но оно имеет место в Федеральном законе "О техническом регулировании" и является базовым в условиях рыночной экономики. Эта методика предусматривает выполнение в автоматизированном режиме простейшего варианта оценки информационных рисков любой компании. Методика COBRA представляет требования ИСО 17799 в виде тематических "вопросников", на которые следует дать ответ в ходе оценки рисков информационных активов и электронных бизнестранзакций компании. Введенные ответы автоматически обрабатываются, и с помощью некоторых правил формируется итоговый отчет с текущими оценками информационных рисков компании и рекомендации по управлению ими.

Другие подобные методики управления рисками позволяют:

• создавать модели информационных активов компании в отношении безопасности;

• классифицировать и оценивать ценности активов;

• составлять списки наиболее значимых угроз и уязвимостей безопасности;

• ранжировать угрозы и уязвимости безопасности;

• обосновывать средства и меры контроля рисков;

• оценивать эффективность/стоимость различных вариантов защиты;

• формализовать и автоматизировать процедуры оценки рисков и управления ими.

Одна из наиболее известных методик этого класса – методика CRAMM, основными целями которой являются:

• формализация и автоматизация процедур анализа и управления рисками;

• оптимизация расходов на средства контроля и защиты;

• комплексное планирование и управление рисками на всех стадиях жизненного цикла информационных систем;

• сокращение времени на разработку и сопровождение корпоративной системы защиты информации;

• обоснование эффективности предлагаемых мер защиты и средств контроля;

• управление изменениями и инцидентами;

• поддержка непрерывности бизнеса;

• оперативное принятие решений по вопросам управления безопасностью.

Методика позволяет определить ценность ресурсов. Этот шаг является обязательным в полном варианте анализа рисков. Ценность физических ресурсов в данном методе определяется ценой их восстановления в случае разрушения. Ценность данных и программного обеспечения определяется в следующих ситуациях:

• недоступность ресурса в течении определенного периода времени;

• разрушение ресурса – потеря информации или ее полное разрушение;

• нарушение конфиденциальности в случаях несанкционированного доступа штатных сотрудников или посторонних лиц;

• ошибки, связанные с передачей информации: отказ от доставки, недоставка информации, доставка по неверному адресу.

Для оценки возможного ущерба используют следующие критерии:

• ущерб репутации организации;

• нарушение действующего законодательства;

• ущерб для здоровья персонала;

• ущерб, связанный с разглашением персональных данных отдельных лиц;

• финансовые потери от разглашения информации;

• финансовые потери, связанные с восстановлением ресурсов;

• потери, связанные с невозможностью выполнения обязательств;

• дезорганизация деятельности.

Приведенная совокупность критериев используется в коммерческом варианте метода. В других версиях совокупность будет иной, например, в государственных организациях добавляются параметры, отражающие такие области, как национальная безопасность и международные отношения.

Для данных и программного обеспечения выбираются применимые к рассматриваемой информационной системе критерии, дается оценка ущерба по шкале от 1 до 10. Затем разрабатываются шкалы для выбранной системы параметров. Они могут выглядеть, например, следующим образом.

Ущерб, нанесенный репутации организации:

2 – негативная реакция отдельных чиновников, общественных деятелей;

4 – критика в средствах массовой информации, не имеющая широкого общественного резонанса;

6 – негативная реакция отдельных депутатов Госдумы, Совета Федерации;

8 – критика в средствах массовой информации, имеющая последствия в виде крупных скандалов, парламентских слушаний, широкомасштабных проверок и т.п.;

10 – негативная реакция на уровне президента и правительства.

Ущерб для здоровья персонала:

2 – минимальный ущерб (последствия не связаны с госпитализацией или длительным лечением);

4 – ущерб среднего размера (необходимость лечения для одного или нескольких сотрудников, но без длительных отрицательных последствий);

6 – серьезные последствия (длительная госпитализация, инвалидность одного или нескольких сотрудников),

9 – гибель людей.

Финансовые потери, связанные с восстановлением ресурсов:

2 – менее 1000 долл.;

6 – от 1000 до 10000 долл.;

8 – от 10000 до 100000 долл.;

10 – свыше 100000 долл.

Дезорганизация деятельности в связи с недоступностью данных:

2 – отсутствие доступа к информации до 15 минут;

4 – отсутствие доступа к информации до 1 часа;

6 – отсутствие доступа к информации до 3 часов;

8 – отсутствие доступа к информации до 12 часов;

10 – отсутствие доступа к информации более суток.

На этапе оценки угроз и уязвимостей определяется зависимость пользовательских услуг от определенных групп ресурсов и существующий уровень угроз и уязвимостей. Уровень угроз, в зависимости от ответов, оценивается как очень высокий; высокий; средний; низкий; очень низкий; уровень уязвимости – в зависимости от ответов, как высокий; средний; низкий. Уязвимость может и вовсе отсутствовать.

**Управление рисками.** На этом этапе CRAMM генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням. Конкретные меры разбиваются на группы и подгруппы по следующим категориям:

- обеспечение безопасности на сетевом уровне;
- обеспечение физической безопасности;
- обеспечение информации поддерживающей инфраструктуры;
- меры безопасности на уровне системного администратора.

Это позволяет получать обоснованные оценки существующих и допустимых уровней угроз, уязвимостей, эффективности защиты. Когда рассматривают риски (например в Британском стандарте BS 7799), считают, что ключевой задачей системы управления ИБ является обследование информационной системы для определения того, какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите. При определении степени риска принято учитывать ценность ресурса, уровень угрозы и степень уязвимости. Из всех этих параметров более или менее точно можно определить первый. И то в системах (сетях) ОП эти величины

сильно отличаются для сообщений разных пользователей. Два других параметра оценить еще более сложно.

Существует и другой подход к оценке затрат на защиту информации от доступа к ее содержанию в сравнении с потерями от успешного проведения атаки. Он основан на рассмотрении информации в качестве ресурса государства, юридического или физического лица. Этот ресурс имеет определенный жизненный цикл. В начале этого цикла информация обладает наибольшей ценностью, но с течением времени она уменьшается. При открытом распространении такой информации ее владелец начинает получать прибыль в период ее наибольшей ценности (Нобу Хау, изобретения, патенты и т.д.). При этом прибыль тем больше, чем больше времени затрачивает злоумышленник на НСД. При ограничении распространения информации возникают расходы на ее защиту и одновременно снижается величина выгоды от ее быстрого использования.

До решения о количественном критерии оценки ИБ можно предложить временное решение: исходить из принципа – угрозы не должны вывести систему из состояния, которое определено нормами на качество услуг инфокоммуникаций, т.е. не испортит основных показателей, указанных выше. Это доставка сообщения по адресу; соблюдение заданного времени передачи информации определенного объема; достоверность; надежность; живучесть. И при этом, не рассчитывая на возможность получения количественных оценок безопасности, использовать оценки типа "удовлетворительно", "лучше пока невозможно" и т.д. Необходимым для этого является наличие в системе связи непрерывного контроля за качеством передачи, как это, например, имеет место в SLA. Такой контроль позволяет судить о появлении угроз, приводящих к засылке информации не по адресу, перегрузке системы, несоблюдению норм по достоверности и времени доставки информации, т.е. по сути дела, обеспечивает мониторинг систем коммутации, управления, ОКС и т.п.

Таким образом, владельцы информации в зависимости от срока доступа к ней имеют, с одной стороны, упущенную выгоду, а с другой, – предотвращенный ущерб. Оценка позитивных и негативных последствий весьма сложна. Поэтому принятие решения по защите информации приходится осуществлять в условиях большой неопределенности. Кроме того, рассмотренный подход имеет недостаток, поскольку оценивается только один вид НСД, а именно, доступ к содержанию информации и не учитываются другие типы угроз.

При этом следует использовать оценки типа "удовлетворительно", "лучше пока не возможно" и т.п.

В ряде публикаций по вопросам ИБ отмечается, что интеллектуальная собственность производственной информации соизмерима со стоимостью и даже дороже стоимости производимой продукции. Естественно возникает вопрос, как оценивать стоимость информации? Известны попытки ответов на этот вопрос. В одной из них ценность информации определяется на основе развитых Р.А. Стратановичем теории информации и теории статистических решений. Ценность информации определяется как мера той максимальной пользы, которую данное количество информации способно принести для уменьшения потерь, сопровождающих функционирование системы. Очевидный недостаток работ такого рода заключается в том, что определенная в них ценность информации не учитывает того обстоятельства, что действительная ценность различна для разных владельцев информации, не говоря уже о злоумышленниках, старающихся получить доступ к ее содержанию.

Общий недостаток всех методик – наличие субъективных оценок на промежуточных этапах и отсутствие количественных оценок состояния ИБ. Изложенные пессимистические оценки ни в коем случае не должны привести к выводу о безуспешности работ по повышению ИБ систем и сетей электросвязи. Наоборот, они должны стимулировать, наряду с практической разработкой методов повышения ИБ и их широким внедрением в практику, интерес к теоретическим аспектам исследо-

вания проблемы. Такой вывод неизбежен, поскольку прогресс электросвязи базируется на успехах микроэлектроники и ПО, и существующее положение в области ИБ является одним из примеров проблемы "щита и меча", "замка и ключа".

**ПРЕДЛОЖЕНИЯ АВТОРА ПО КОЛИЧЕСТВЕННЫМ ХАРАКТЕРИСТИКАМ ЗАЩИЩЕННОСТИ СИСТЕМ (СЕТЕЙ) СВЯЗИ ОТ ВИРУСНЫХ АТАК И СПАМА**

Учитывая отсутствие общепринятой количественной характеристики степени ИБ, наберемся смелости предложить в качестве паллиативного решения следующее. Принцип предлагаемой оценки величины ИБ для наиболее опасной (как в отношении частоты появления, так и поражающей способности) причиной поражения ИБ основывается на том, что вирусы нарушают все три характеристики качества услуг: достоверность, доставка по адресу, время доставки сообщений.

В качестве характеристик для вирусов и спама предлагаются коэффициенты готовности по вирусам  $K_{ГВ}$  и спаму  $K_{ГС}$ . Такая характеристика по вирусам позволяет сравнивать степень ИБ системы (сети) в зависимости от параметров наиболее популярного вида защиты услуг от вирусов с помощью межсетевых экранов. Эффективность защитного действия экрана определяется двумя его параметрами: временем (частотой) обновления антивирусных программ  $T_0$  и временем, затрачиваемым на замену программ,  $T_3$ . Принято, что эффективность защитного эффекта экрана обратно пропорциональна величине этих параметров и предлагается следующее выражение зависимости  $K_{ГВ}$  от значений  $T_0$  и  $T_3$ :

$$K_{ГВ} = (1/T_0)/(T_0 + T_3).$$

В настоящее время в наиболее совершенных экранах смена антивирусных программ ( $T_0$ ) осуществляется автоматически с периодом от одних суток до одного часа, а время замены программ ( $T_3$ ) составляет от одной до 20 минут.

Значения  $K_{ГВ}$ , рассчитанные по приведенной формуле для некоторых  $T_0$  и  $T_3$ , показаны в табл. 2.

Из табл. 2 следует, что наибольший  $K_{ГВ}$  достигает значения 0,985 при малых  $T_0$  и  $T_3$  и мало зависит от значения последнего. Наименьшие  $K_{ГВ}$  имеют место при больших  $T_0$  и  $T_3$  и составляют 0,545. Данные таблицы позволяют судить, насколько эффективно межсетевые экраны с разными характеристиками  $T_0$  и  $T_3$  защищают системы (сети) связи от вирусных атак. Это позволяет сделать вывод относительно адекватности системы защиты действию угроз ИБ путем нахождения соотношений между затратами на защиту и ее эффективностью.

Несколько иной подход предлагается для оценки опасности спама. Дело в том, что спам влияет на величину доступности пользователя к системе связи, которая может быть определена экспериментально в виде процента времени недоступности. В основу этой методики предлагается положить процент спама в получаемой информации. Очевидно, чем больше этот процент, тем меньше  $K_{ГС}$ .

Для определения  $K_{ГС}$  предлагается такое соотношение:

$$K_{ГС} = 1 / \left( 1 + \frac{\text{процент спама}}{100} \right).$$

Расчет показывает, что при 80% спама  $K_{ГС} = 0,555$ ; при 40%  $K_{ГС} = 0,714$ ; при 10%  $K_{ГС} = 0,91$ .

Таким образом,  $K_{ГС}$  характеризует вероятность отказов в установлении соединения и эффективность защиты от спама различных типов антиспамеров и тем самым позволяет оценить степень адекватности защиты системы связи от интенсивности атак спама. Подобного рода характеристики

широко применяются для оценки надежности различных систем, в том числе систем и сетей связи. Поэтому пользователи привыкли характеризовать величину надежности числом дефяток после запятой. Необходимо иметь в виду, что между надежностью системы (сети) связи и ее живучестью существует различие. Оно заключается в том, что между источниками помех и искажений в теории надежности фигурируют стационарные случайные процессы, а в теории ИБ - нестационарные, поскольку злоумышленник ставит перед защитой ИБ все новые и новые задачи. Именно поэтому и потому, что случайные со вторыми столкнулись значительно позже, чем с первыми, стационарные случайные процессы лучше изучены теоретически и экспериментально.

Как отмечено в "Доктрине информационной безопасности РФ", система обеспечения ИБ РФ является частью системы обеспечения национальной безопасности страны. В свою очередь система обеспечения безопасности систем и сетей связи является частью системы обеспечения информационной безопасности, а защита информации – технологией процесса обеспечения ИБ и систем (сетей) связи.

В настоящее время по вопросам информационной безопасности имеется много законов и подзаконных актов, издано большое количество книг, статей, руководств и стандартов, содержащих полезные сведения по угрозам ИБ и методам защиты от них. Это создает в ряде случаев некоторую самоуспокоенность в отношении состояния дел с ИБ. Мне могут возразить, что такое положение имеет место во всем мире. Наше же положение значительно хуже, так как мы не только строим системы (сети) в основном на импортном оборудовании, но и используем зарубежные технологии для защиты ИБ. Кроме того, возникает вопрос: не обладают ли зарубежные организации более совершенной системой защиты, но не торопятся ознакомить нас с ней?

Представляется, что на разработке количественной характеристики состояния ИБ следует сконцентрировать усилия высококвалифицированных специалистов в области защиты систем (сетей связи) – математиков, компьютерщиков, разработчиков аппаратуры связи и создателей устройств защиты и их ПО. Несмотря на сложность поставленной задачи и для ее решения уже многое сделано, однако результаты, которые можно практически использовать, отсутствуют. Естественно, эта задача должна решаться одновременно с обеспечением нашей независимости от иностранных производителей в отношении устройств связи, защиты и ПО.

**ОСОБЕННОСТИ ХАРАКТЕРИСТИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Обеспечение информационной безопасности характеризуется: важностью; сложностью; высокой степенью ответственности. Ее важность определяется той огромной ролью, которую играют системы информатизации и, следовательно тем, насколько важно обеспечивать их безопасность.

Сложность обеспечения ИБ систем (сетей) связи ОП в России обуславливается рядом причин:

- громадной протяженностью каналов;
- разнообразием устанавливаемых и работающих систем передачи, коммутации, управления;
- наличием двух групп операторов: основных и альтернативных;
- большим разнообразием услуг;
- разнообразием требования пользователей к НСД.

Вместе с тем архитектура системы безопасности должна быть единая и используемые в ней технологии защиты от НСД должны быть совместимы.

Как и в отношении каждой большой системы, естественно возникает вопрос, как строить систему безопасности страны

Таблица 2

$\frac{T_0, \text{ч}}{T_3, \text{м}}$	$\frac{1}{1/60}$	$\frac{1}{1/30}$	$\frac{1}{1/10}$	$\frac{6}{1/10}$	$\frac{6}{1/5}$	$\frac{6}{1/2}$	$\frac{12}{1/5}$	$\frac{12}{1}$	$\frac{12}{10}$	$\frac{24}{1}$	$\frac{24}{10}$	$\frac{24}{20}$
$K_{ГВ}$	0,975	0,970	0,910	0,993	0,969	0,923	0,985	0,923	0,545	0,960	0,685	0,545

(централизованно, децентрализованно, комбинированно)? С одной стороны, создать единую централизованную систему обеспечения безопасности для всей страны очень трудно. С другой стороны, путь децентрализованного создания систем в отдельных сетях и системах, у отдельных операторов и в отдельных регионах контрпродуктивен, так как при этом трудно, а может быть и невозможно обеспечить проведения единой технической политики безопасности. По-видимому, нужно идти путем обеспечения сопряжения отдельных систем (сетей) электросвязи на основе единой архитектуры безопасности и единых требований к технологиям защиты, обеспечивающим единые интерфейсы на стыках частных систем (сетей). Для обеспечения такого единства в каждой системе (сети) связи должно быть лицо, отвечающее за все вопросы безопасности передачи информации.

Особенно необходимо иметь в виду то, что отдельные каналы и тракты системы (сети) связи ОП в ряде случаев используются для передачи конфиденциальной информации корпоративных систем (сетей). В этих случаях содержание и трафик информации ограниченного пользования владельцами корпоративных систем (сетей) защищаются от НСД криптографическими методами. Но наличие в системах (сетях) такой информации накладывает требования к системам (сетям) ОП, поскольку в последних существуют подсистемы и устройства, являющиеся общими для открытий и конфиденциальной информации.

Вредоносные воздействия на эти подсистемы и устройства приводят к нарушению их нормального функционирования, что отрицательно сказывается на передаче информации не только общего пользования, но и конфиденциальной. В связи с этим в системах (сетях) связи ОП необходима организация защиты от вредоносных влияний на все групповые подсистемы и общие устройства. Высокая степень ответственности решения вопросов ИБ систем связи вызвана следующими причинами:

- тот, кто берется за обеспечение ИБ возлагает на себя огромную ответственность, особенно в условиях, когда отсутствует количественная мера степени ИБ;
- наличием нерешенных вопросов, как в теории, так и на практике в области ИБ;
- большим объемом сложных задач разработки и внедрения систем ИБ.

Вот почему при решении вопросов обеспечения ИБ в нашей стране сферы ответственности распределены между государственными органами и другими организациями. Закон "О связи" (2003 г.) в Статье 12 определяет, что "федеральный орган исполнительной власти в области связи устанавливает требования к сетям электросвязи ОП в отношении их защиты от НСД и передаваемой посредством их информации". Согласно "Положению о Министерстве информационных технологий и связи РФ" (2004 г.) это министерство определено как федеральный орган исполнительной власти, осуществляющий функции по выработке государственной политики и нормативно-правовому регулированию в сферах информационных технологий и электросвязи. Согласно Статье 7 закона "О связи" "Сети связи и сооружения связи находятся под защитой государства. Операторы и застройщики при строительстве и реконструкции сетей и сооружений связи должны учитывать необходимость их защиты от НСД. Операторы связи при эксплуатации сетей и сооружений связи обязаны обеспечивать их защиту от НСД". Согласно "Положению о Федеральном агентстве связи и его полномочиях входит: "размещение заказов на проведение научно-исследовательских работ для государственных нужд в установленной сфере деятельности".

Таким образом, Мининформсвязь и его Федеральное агентство связи отвечают за политику и требования к системам и сетям связи в отношении их защиты от НСД и передаваемой по ним информации, а также размещают заказы на выполнение НИР для государственных нужд в области связи. Заметим, что министерство отвечает за возложенные на него функции в отношении всех систем и сетей связи, тогда как Федеральное

агентство – только за работы, выполняемые для государственных нужд.

Тем не менее, желательно ускорить разработку подзаконных актов и правил, руководств, инструкций и стандартов, которые в соответствии с принятой политикой ИБ РФ содержали бы рекомендации по архитектуре систем ИБ РФ. Эти материалы должны охватывать весь комплекс работ по созданию систем ИБ, начиная от выдачи заданий на проектирование систем (сетей) связи ОП, содержать требования к техническому обеспечению ИБ и экономическому обоснованию принимаемых решений, описывать порядок приемки заказчиком выполненных проектов.

В разрабатываемых проектах должны обязательно содержаться методики выявления уязвимых мест в системе ИБ и планы действий эксплуатационного персонала в случаях взлома защиты и необходимости восстановления утерянных данных. Проекты должны обеспечивать максимальную надежность решения защиты и наибольшую эффективность рекомендуемых технологий, которые достигаются создаваемыми системами управления ИБ и проведением регулярного контроля их состояния в процессе эксплуатации.

Все мероприятия проектов должны предусматривать их поддержку со стороны эксплуатационного персонала, без которой все они не могут работать с полной отдачей.

Эксплуатационные организации совместно со строительными должны реализовывать все рекомендации проектов в отношении ИБ при создании и реконструкции систем (сетей) связи.

Заметим, что в США разработкой стандартов по безопасности в области телекоммуникаций занимаются на весьма высоком уровне. Это – консультативный комитет по связи в системе национальной безопасности США (NSTAC) и Совет по надежности и взаимодействию сетей Федеральной комиссии по связи США (FCC NRIC). Кроме того, разработчики и эксплуатационный персонал, ответственные за безопасность информационных систем, проходят сертификацию по безопасности, одобренную Международным консорциумом сертификации по безопасности компьютерных систем (ISCZ). По-видимому, необходимо подумать о использовании подобной практики и в нашей стране.

Так как эксплуатация систем и эксплуатация сетей связи часто осуществляются разными организациями (операторами систем и операторами сетей), то естественно возникает вопрос, за что отвечают первые и вторые. За ИБ сетей отвечают операторы сетей связи. Соответственно за безопасность систем должны отвечать операторы систем. Такое разделение ответственности соответствует прогрессивной технологии обеспечения качества услуг SLA в части ИБ и должно быть утверждено в соответствующем подзаконном акте. Это очень важно потому, что технология SLA предусматривает единоличную ответственность за качество услуг головного оператора системы связи, т.е. того оператора, с которым пользователь имеет договор на предоставление услуг.

Помимо этого подзаконным актом должны быть определены взаимоотношения в области ИБ между операторами сетей связи ОП и операторами присоединяемых сетей, по которым зачастую передается информация, доступ к которой ограничен.

#### НЕКОТОРЫЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ (СЕТЕЙ) СВЯЗИ ОП

В нашей стране существует много директивных документов, определяющих политику Российской Федерации в области ИБ. В этих документах определены официальные взгляды на проблему ИБ РФ и сформулированы предложения по совершенствованию научно-технического, методического, правового и организационного обеспечения ИБ. Рассмотрены и систематизированы виды угроз ИБ, методы и системы защиты от этих угроз. Определены задачи и направления работ в области политики систем ИБ. Политика ИБ страны базируется

на законах РФ и подзаконных актах, а также на рекомендациях МСЭ, ETSI, ИСО и стандартах, как отечественных, так и зарубежных.

Информационная безопасность – такая область, в которой невозможно обойтись без отечественных разработок в части обеспечения защиты сетей и систем связи.

Отечественная наука обеспечения ИБ систем (сетей) связи имеет большие достижения в разработке средств защиты от вирусов и спама. Например, "Лаборатория Касперского" достигла возможности предугадывать тенденции развития вирусов и заблаговременно отражать будущие атаки злоумышленников. Многие зарубежные разработчики в своих продуктах ПО используют антивирусы Касперского.

К настоящему времени у нас в стране хорошо изучены все виды угроз ИБ, направления (цели) их атак, уязвимые места систем (сетей). Разработаны методы защиты от угроз всех видов, а также системы предварительного определения и предотвращения угроз. Все это свидетельствует, с одной стороны, об имеющихся успехах в области ИБ в нашей стране, а с другой создает настроение самоуспокоенности, уверенности в том, что положение с ИБ систем (сетей) связи ОП вполне благополучно. Однако в отношении степени обеспечения необходимой ИБ имеются серьезные проблемы, что не позволяет остановиться на достигнутом. Важнейшими из этих проблем представляются следующие:

- широкое использование в действующих системах (сетях) связи ОП аппаратно-программных устройств, которые подвержены угрозам со стороны злоумышленников.

- широкое использование зарубежных устройств защиты от угроз;

- широкое использование программируемых устройств в системах защиты информации от угроз, также являющихся целью атак злоумышленников.

По данным Форума "Технологии безопасности", 70–73% специалистов считает необходимым ограничить допуск на российский рынок средств защиты информации оборудования зарубежных фирм и только 15% специалистов полагают, что такой допуск необходим. Мы присоединяемся к мнению первых. По этой же причине возникает угроза ИБ, вызываемая возможностью наличия в закупаемом оборудовании вредоносных закладок. Правда обязательное применение в системах передачи и защиты информации только сертифицированных ФСБ и ФСТЭК изделий сводит опасность закладок к минимуму. О степени же влияния всех этих угроз на реальную ИБ говорить затруднительно.

Эта неопределенность является следствием отсутствия количественной характеристики степени защищенности системы (сети) в отношении ИБ. Конечно нельзя не учитывать несомненную пользу, которую приносит существующая система защиты от угроз. Однако, недостаточность такой защиты, несмотря на большие затраты на средства защиты и их эксплуатацию, может привести к труднооценимым последствиям. Ведь к сетям ОП присоединены многочисленные корпоративные сети, по которым часто передается конфиденциальная информация. Отсутствие или недостаточная защита сетей ОП от угроз злоумышленников вызывает возможность нарушения нормального функционирования устройств или подсистем общих для всех или части каналов связи. К числу таких устройств относятся мультиплексоры, усилители, регенераторы, коммутаторы, маршрутизаторы, а к числу подсистем: управление, мониторинг, сигнализация, контроль и т.п.

Нарушение нормального функционирования этих устройств и подсистем сказывается на качестве передачи и работоспособности всех или множества каналов, в том числе и тех, по которым передается конфиденциальная информация. Важность этой информации и отрицательные последствия, к которым могут привести такие нарушения, подтверждается необходимостью защиты систем (сетей) ОП от вредоносного влияния злоумышленников. Поэтому необходимо включить в правила, где рассматриваются взаимоотношения между про-

вайдерами корпоративных сетей и сетей ОП, дополнения в отношении обеспечения ИБ.

Нельзя не обратить внимание на то, что широкое использование аппаратуры передачи и устройств защиты зарубежного производства является нарушением закона "О связи", согласно которому "все участники Телекоммуникационного рынка, начиная с 1999 г. обязаны обеспечить приоритет производства средств связи и применения в эксплуатации произведенных в РФ средств связи".

Кроме вышеизложенных основных проблем обеспечения ИБ систем (сетей) связи ОП имеется ряд частных вопросов, нуждающихся в дополнительной проработке, и применении ряда методик, таких как:

- определение политических, экономических и моральных последствий реализации угроз ИБ из-за отсутствия или недостаточной эффективности системы защиты информации;

- определение стоимости создания и эксплуатации систем обеспечения ИБ;

- обеспечение ИБ мобильных систем (сетей) передачи информации;

- защита ИБ системы оперативно-розыскных мероприятий (СОРМ);

- защита ИБ систем (сетей) доступа и структурированных систем внутри зданий;

- интеграция систем управления функционированием служб и сетей передачи с системами управления ИБ.

**Конечно, этими проблемами и вопросами далеко не ограничивается необходимость целенаправленной работы по обеспечению надежной ИБ систем (сетей) связи ОП. Но, как представляется, рассмотренные проблемы и вопросы являются на сегодня наиболее принципиальными и первоочередными, и именно на них следует сосредоточить усилия коллективов научных, опытно-конструкторских организаций и заводов-изготовителей оборудования систем (сетей) связи ОП.**