Вестник УГАТУ
Уфа : УГАТУ, 2011 Т. 15, № 5 (45). С. 66–72

УДК 004.2

И. Л. Виноградова, М. Н. Даннави

ТРЕБОВАНИЯ К СИСТЕМЕ ТРАНСПОРТИРОВКИ СООБЩЕНИЙ ОБЩЕЙ КАНАЛЬНОЙ СИГНАЛИЗАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Статья посвящена исследованию возможности применения вероятностной модели исходов, возможных при решении обобщенных функций обеспечения безопасности информации. Рассмотренные методы обоснования требований к системе обеспечения безопасности информации позволяют в общих чертах определить характеристики структуры проектируемой системы защиты и применяемых методов обеспечения безопасности информации, однако не позволяют обосновать значения количественных характеристик разрабатываемых систем. Этот недостаток отсутствует при использовании методов на основе анализа степени риска и вероятностной модели. *Сети связи общего пользования (ССОП)*; *система обеспечения безопасности информации (СОБИ)*; *несанкционированный доступ (НСД)*; *общая канальная сигнализация № 7*; *система контроля доступа (СКД)*

ВВЕДЕНИЕ

Обоснование требований – первоочередная и основополагающая задача проектирования систем защиты информации, поскольку результаты ее решения составляют исходную базу для реализации всех последующих этапов жизненного цикла системы.

В настоящее время существует несколько основных подходов к обоснованию требований к системам защиты:

- на основе классификации систем, входящих в состав сетей связи общего пользования (ССОП) [2];
- на основе специфики технологии автоматизированной обработки информации [3];
- на основе анализа степени риска [4, 5];
- на основе вероятностной модели исходов, возможных при решении обобщенных функций обеспечения безопасности информации [3].

При первом методе обоснования требований учитывается тот факт, что сети связи общего пользования могут состоять из нескольких компонентов, которые выполняют частные задачи и, в общем случае, может быть ориентированы на различные уровни защиты информации. Поэтому при обосновании требований к системе защиты выполняется четкая классификация средств автоматизации, входящих в состав сеть связи общего пользования. Эта классификация основывается на перечне защищаемых информационных ресурсов и уровнях их конфиденциальности, описании организационной структуры подразделений, использующих автоматизированные системы, условиях их функционирования, а также на характеристиках возможных режимов обработки данных. При этом система требований формируется на базе классификатора уровней защищенности. Всего выделяется семь уровней, причем каждый более высокий уровень включает все требования более низких уровней.

Второй метод предполагает, что для повышения полноты и объективности обоснования требований в конкретной ситуации целесообразно разработать развитую систему рекомендаций, учитывающих современные возможности и условия автоматизированной обработки информации. В основе системы рекомендации лежит утверждение, что конкретные требования к системе обеспечении безопасности информации, обусловленные спецификой автоматизированной обработки информации, определяются совокупностью следующих факторов: характером обрабатываемой информации; объемом обрабатываемой информации; продолжительностью пребывания информации в системе; технологией обработки информации; организацией информационно-вычислительного процесса; этапом жизненного цикла системы.

В качестве примера разработки такой системы рекомендации рассмотрим обоснование требований с учетом первого фактора – характера обрабатываемой информации. По характеру (с точки зрения защиты) информацию можно разделить на общедоступную, конфиденциальную (личную, персональную), служебную, секретную и совершенно секретную. Можно предложить следующие рекомендации по предъявлению требований к защите:

1. При обработке общедоступной информации никаких специальных мер защиты от несанкционированного доступа не требуется.

Контактная информация: (347) 272-43-84

2. Требования к защите конфиденциальной информации определяет пользователь, устанавливающий статус конфиденциальности;

3. При обработке информации с грифом «Для служебного пользования» (и соответствующего ему) к ней должен быть обеспечен свободный доступ пользователей учреждения – владельца этой информации (по общему списку); доступ же пользователей, не включенных в общий список, должен осуществляться по разовым санкциям, выдаваемым администратором системы;

4. Информация с грифом «Секретно» в зависимости от ее объема и характера может предоставляться в одном из следующих вариантов:

- персональное разграничение – для каждого элемента информации составляется список пользователей, имеющих право доступа к нему;
- коллективное разграничение – структура баз защищаемых данных организуется в соответствии со структурой подразделений, участвующих в обработке защищаемой информации. При этом пользователи каждого подразделения имеют право доступа только к «своим» данным;

5. При обработке информации с грифом «Совершенно секретно» список лиц, имеющих право доступа, должен составляться для каждого самостоятельного элемента информации с указанием дней и времени доступа, а также перечня разрешенных процедур.

Рассмотренные методы обоснования требований к системе обеспечения безопасности информации позволяют в общих чертах определить характеристики структуры проектируемой системы защиты и применяемых методов обеспечения безопасности информации, однако не позволяют обосновать значения количественных характеристик разрабатываемых систем. Этот недостаток отсутствует при использовании методов на основе анализа степени риска и вероятностной модели.

ДИАГРАММА РИСКА НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В СЕТЯХ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ

Анализ степени риска проводится для определения возможных потерь в случае нарушения безопасности информации. Существующие методы анализа предполагают разработку специализированных шкал оценки допустимых потерь в различных единицах измерения (чаще всего используются шкалы, привязанные к финансовым потерям). Упрощенная диаграмма анализа риска изображена на рис. 1.

Получение количественных оценок степени риска основывается на введении специальных показателей, характеризующих возможные потери для каждого типа угроз безопасности информации. В частности, могут использоваться коэффициенты ожидаемых потерь и пороговые значения допустимых потерь.

Превышение допустимых потерь обосновывает требования по использованию дополнительных мер и средств защиты.

Обоснование соответствия между допустимыми потерями и стоимостью выбранного для каждого сценария нарушения безопасности информации варианта защиты выполняется с учетом стоимости введения средств защиты, планируемого времени их применения и стоимости эксплуатации.

Основная сложность применения этого метода для обоснования требований к системам защиты в структурно сложных сетях заключается в определении пороговых значений допустимых потерь, так как очень трудно оценить количественно потери от компрометации информации.

Сущность метода обоснования требований к системам защиты на основе вероятностной модели исходов заключается в определении функций защиты информации, обеспечивающих выполнение следующих условий:

- в процессе функционирования сети связи общего пользования должны быть реализованы такие мероприятия, при которых невозможно проявление дестабилизирующих факторов;
- при проявлении дестабилизирующих факторов они будут обнаружены средствами системы обеспечения безопасности информации;
- даже если дестабилизирующие факторы имели место и не обнаружены, их последствия будут локализованы и ликвидированы средствами системы обеспечения безопасности информации.

Полученное множество функций является основой при обосновании требований к структуре системы обеспечения безопасности информации, так как каждая функция защиты должна реализовываться определенной совокупностью средств защиты информации.

Следующим этапом метода является построение вероятностной модели исходов реализации выбранного множества функций защиты

и доказательства его полноты. Полученная модель является средством обоснования требований к характеристикам и оптимизации системы обеспечения безопасности информации. Это обусловлено тем, что осуществление функций защиты информации сопряжено с расходованием тех или иных ресурсов. Поэтому уровень осуществления каждой из функций защиты при прочих равных условиях зависит от количества расходуемых ресурсов и задачу обоснования требований к характеристикам системы защиты можно сформулировать как оптимизационную задачу двух видов:

- требуется найти характеристики системы обеспечения безопасности информации, обеспечивающие при минимальных затратах достижение заданного уровня защищенности информации (прямая задача);
- требуется найти характеристики системы обеспечения безопасности информации, при которых обеспечивается достижение максимально возможного уровня защищенности информации при заданных затратах на создание данной системы.

Основная сложность при использовании данного метода заключается в формировании исходных данных для расчета, которые могут быть получены как на основе долговременного сбора статистической информации и ее последующей обработки, так и методами испытаний. Однако, несмотря на это, рассмотренный метод обоснования требований на основе вероятностной модели позволяет со значительной степенью достоверности формализовать процесс функционирования системы обеспечения безопасности информации и определить ее характеристики. В настоящее время рассмотренный метод широко апробирован при обосновании требований к комплексным системам обеспечения безопасности информации [3].

Таким образом, анализ современных методов обоснования требований к системам защиты позволяет сделать вывод, что наиболее эффективным является метод на основе вероятностной модели исходов.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА К РЕСУРСАМ СЕТЕЙ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ

Исследование методов и средств контроля доступа к ресурсам сети связи общего пользования относится по своему содержанию к классу методически сложных задач, в которых наряду с вопросами чисто технологического характера, возникающими на этапе разработки системы контроля доступа, изучаются модели воздействия нарушителя с целью преодоления системы защиты и получения несанкционированного доступа к защищаемой информации, а также оцениваются последствия таких воздействий при выполнении системой своих функциональных задач. Сложность проведения исследований в данной области обусловлена, главным образом, неопределенностью, связанной с развитием технических и программных средств доступа к информации потенциальными нарушителями и возможностью появления новых способов, методов и реализующих их средств.

При обосновании структуры и характеристик системы контроля доступа необходимо рассматривать принципы формирования модели угроз безопасности информации и потенциальные попытки осуществления несанкционированного доступа.

При исследовании методов и средств контроля доступа к ресурсам сети связи общего пользования учитываются факторы, имеющие в большинстве случаев случайный характер. Следовательно, показатели эффективности тех или иных методов контроля доступа лучше всего выражать вероятностной мерой, а для их вычисления использовать вероятностную модель исходов, возможных при решении обобщенных задач предотвращения несанкционированного доступа к ресурсам сети связи общего пользования (рис. 2, табл. 1).

Разработка такой модели основывается на методике, приведенной в [3], в соответствии с которой безопасность информации будет обеспечена, если в процессе функционирования системы контроля доступа созданы следующие условия:

- в процессе функционирования системы выполнены мероприятия, делающие невозможным несанкционированный доступ к защищаемым ресурсам;
- при обнаружении попыток нарушения установленных правил доступа к ресурсам сети связи общего пользования они будут локализованы и предотвращены средствами системы контроля доступа;
- даже если попытки несанкционированного доступа к ресурсам сети связи общего пользования имели место и не обнаружены, их последствия будут локализованы и ликвидированы средствами системы контроля доступа.

Из представленной модели видно, что одиннадцать пронумерованных итоговых событий составляют полную группу, причем события в группе несовместны.

Из теории вероятностей известно, что сумма вероятностей событий такой группы равна единице. Тогда сумма вероятностей первых шести событий есть вероятность того, что безопасность информации при применении разрабатываемой системы контроля доступа обеспечена. Так как все итоговые события являются случайными и составляют полную группу несовместных событий, то

$$\sum_{i=1}^{11} P_i(t) = 1,$$

где $P_i\{t\}$ – вероятность i-го итогового события на заданном интервале времени t.

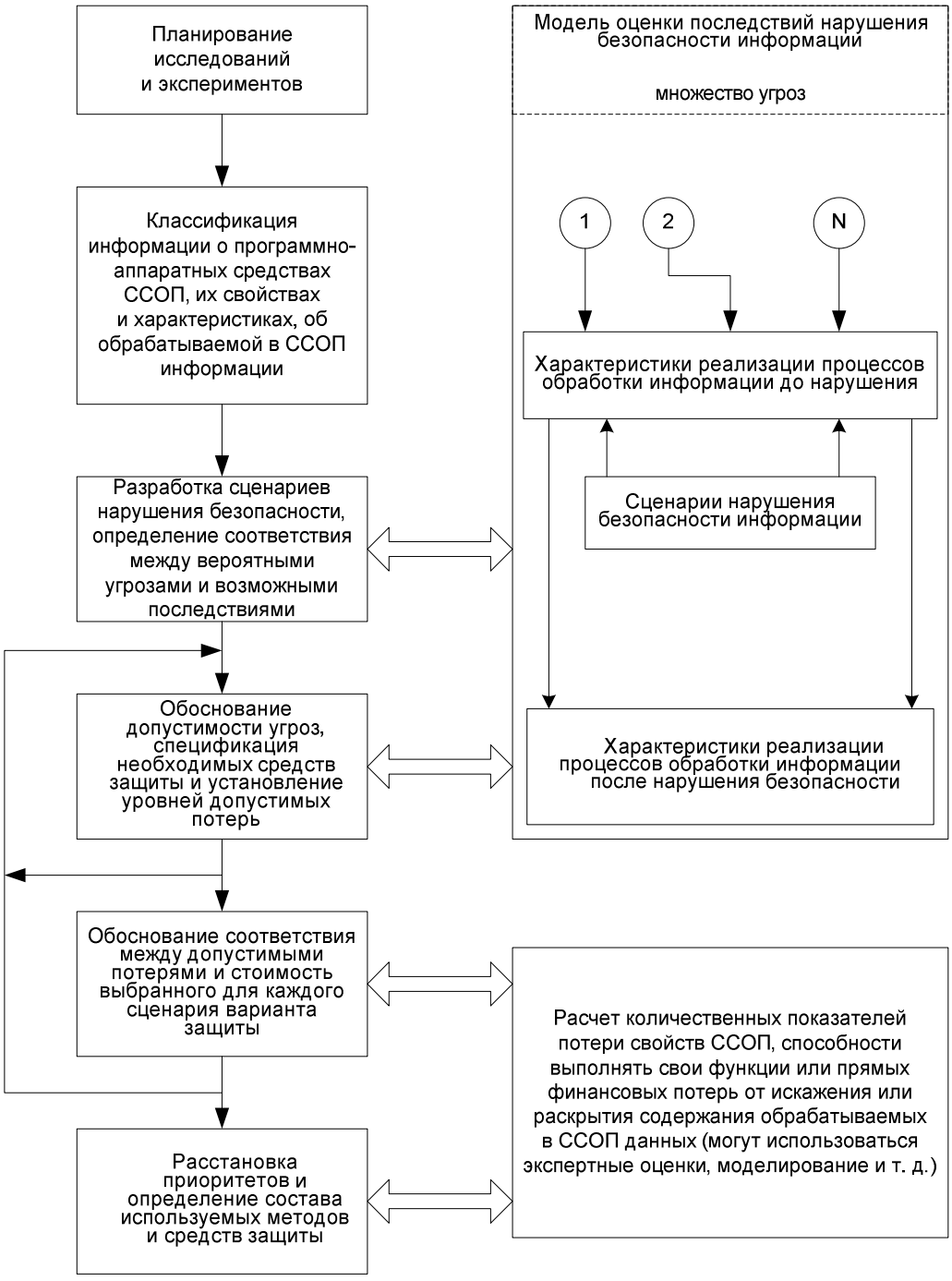

Рис. 1. Упрощенная диаграмма риска

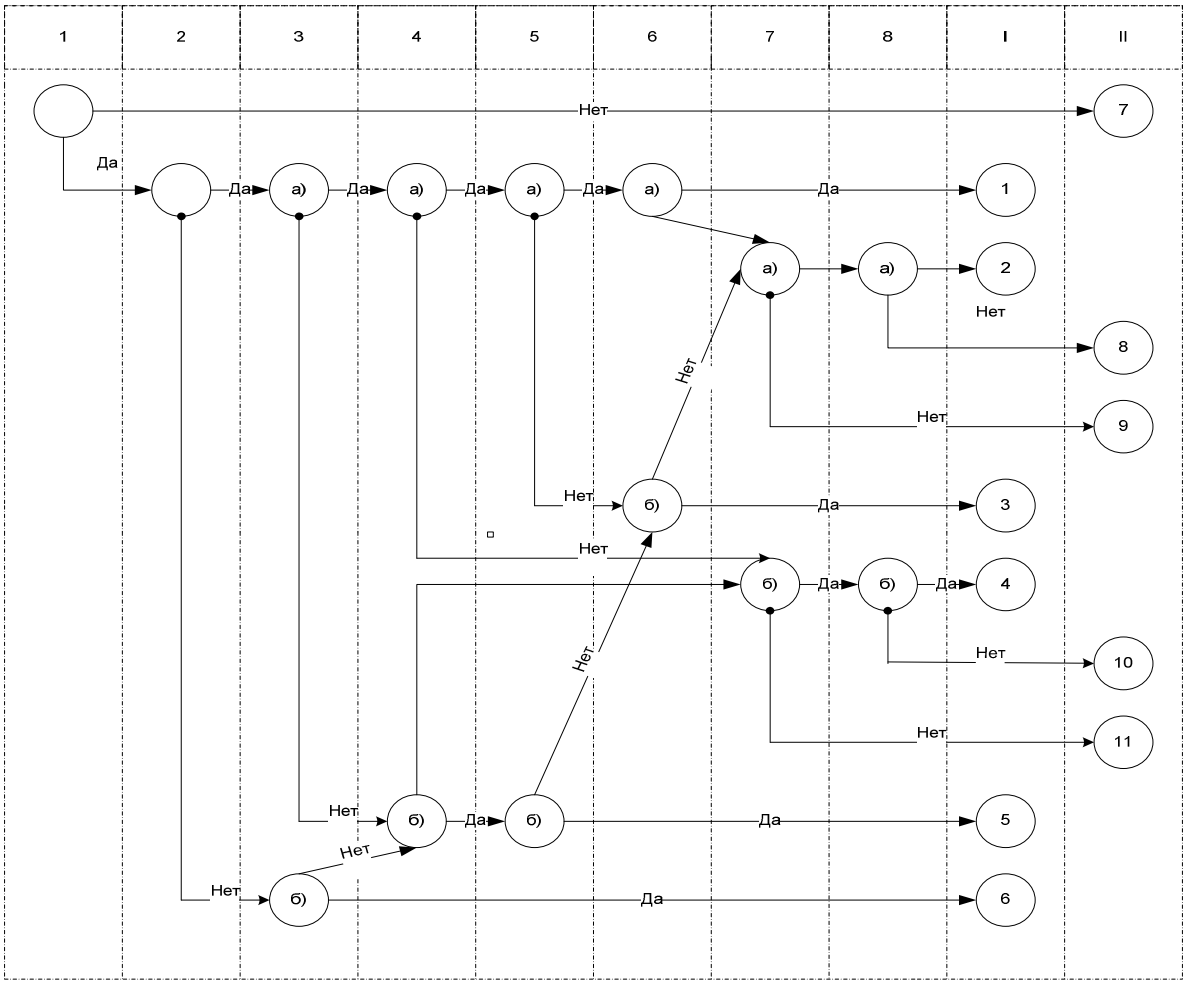

Рис. 2. Вероятностная модель системы контроля доступа:
I – несанкционированный доступ к ресурсам предотвращен;
II – несанкционированный доступ к ресурсам не предотвращен

Функция системы контроля доступа
1. Предотвращение несанкционированного доступа на уровне авторизации ресурсов сети связи общего пользования
2. Предотвращение попыток несанкционированного доступа первого типа
3. Предотвращение попыток несанкционированного доступа второго типа: а) нарушителя класса 2.1; б) нарушителя классов 2.2 и 2.3
4. Предотвращение попыток несанкционированного доступа третьего типа: а) нарушителя класса 3.1; б) нарушителя классов 3.2, 3.3 и 3.4
5. Предотвращение попыток несанкционированного доступа четвертого типа: а) нарушителя классов 4.1, 4.4 и 4.6; б) нарушителя классов 4.2, 4.3 и 4.5
6. Предотвращение попыток несанкционированного доступа пятого типа: а) нарушителя классов 5.1 и 5.5; б) нарушителя классов 5.2, 5.3, 5.4, 5.6, 5.7 и 5.8
7. Обнаружение попыток несанкционированного доступа на уровне аудита: а) информационных потоков при межсетевом взаимодействии; б) выполняемых операций с ресурсами без межсетевого взаимодействия
8. Локализация и ликвидация несанкционированного доступа: а) информационных потоков при межсетевом взаимодействии; б) выполняемых операции с ресурсами без межсетевого взаимодействия

В этом случае можно определить вероятность наступления итоговых событий, каждое из которых вычисляется с помощью следующих выражений:

$$P_1(t) = P_a(t) \cdot P_{u1}(t) \cdot P_{u21}(t) \cdot P_{u31}(t) \cdot P_{u41}(t) \cdot P_{u51}(t),$$

где $P_a(t)$ – вероятность предупреждения несанкционированного доступа при авторизации информационно-вычислительных ресурсов сети связи общего пользования;

$P_{u1}(t)$ – вероятность предупреждения попытки несанкционированного доступа первого типа;

$P_{u21}(t)$ – вероятность предупреждения попытки несанкционированного доступа второго типа для класса нарушителя 2.1;

$P_{u31}(t)$ – вероятность предупреждения попытки несанкционированного доступа третьего типа для класса нарушителя 3.1;

$P_{u41}(t)$ – вероятность предупреждения попытки несанкционированного доступа четвертого типа для классов нарушителя 4.1, 4.4 и 4.6;

$P_{u51}(t)$ – вероятность предупреждения попытки несанкционированного доступа пятого типа для классов нарушителя 5.1 и 5.5;

$$P_2(t) = P_a(t)\left[\begin{array}{l} P_{u1}(t)P_{u21}(t)P_{u31}(t)P_{u41}(t)\left(1-P_{u51}(t)\right)+ \\ +\left[\begin{array}{l} P_{u1}(t)P_{u21}(t)P_{u31}(t)(1-P_{u41}(t))+ \\ +\left[\begin{array}{l} P_{u1}(t)(1-P_{u21}(t))+ \\ +(1-P_{u1}(t))(1-P_{u22}(t)) \end{array}\right]\times \\ \times P_{u32}(t)(1-P_{u42}(t)) \end{array}\right]\times \\ \times(1-P_{u52}(t)) \end{array}\right]\times$$

$$\times P_{a1}(t)P_{l1}(t),$$

где $P_{u22}(t)$ – вероятность предупреждения попытки несанкционированного доступа второго типа для классов нарушителя 2.2 и 2.3;

$P_{u32}(t)$ – вероятность предупреждения попытки несанкционированного доступа третьего типа для классов нарушителя 3.2, 3.3 и 3,4;

$P_{u42}(t)$ – вероятность предупреждения попытки несанкционированного доступа четвертого типа для классов нарушителя 4.2, 4.3 и 4,5;

$P_{u52}(t)$ – вероятность предупреждения попытки несанкционированного доступа пятого типа для классов нарушителя 5.2, 5.3, 5.4, 5.6, 5.7 и 5.8;

$P_{a1}(t)$ – вероятность обнаружения попытки несанкционированного доступа на уровне аудита информационных потоков при межсетевом взаимодействии;

$P_{l1}(t)$ – вероятность локализации и ликвидации несанкционированного доступа при выполнении операций над ресурсами при межсетевом взаимодействии;

$$P_3(t) = P_a(t)\left[\begin{array}{l} P_{u1}(t)P_{u21}(t)P_{u31}(t)(1-P_{u41}(t))+ \\ +(P_{u1}(t)(1-P_{u21}(t))+(1-P_{u1}(t))\times \\ \times(1-P_{u22}(t)))P_{u32}(t)(1-P_{u42}(t)) \end{array}\right]P_{u52}(t),$$

$$P_4(t) = P_a(t)\cdot\left[\begin{array}{l} P_{u1}(t)P_{u21}(t)(1-P_{u31}(t))+ \\ +\left[\begin{array}{l} (P_{u1}(t)(1-P_{u21}(t))+(1-P_{u1}(t))\times \\ \times(1-P_{u22}(t))) \end{array}\right]\times \\ \times(1-P_{u32}(t)) \end{array}\right]\times$$

$$\times P_{a2}(t)\cdot P_{l2}(t),$$

где $P_{a2}(t)$ – вероятность обнаружения попытки несанкционированного доступа на уровне аудита при выполнении операций над ресурсами без межсетевого взаимодействия;

$P_{l2}(t)$ – вероятность локализации и ликвидации несанкционированного доступа при выполнении операций над ресурсами при межсетевом взаимодействии;

$$P_5(t) = P_a(t)\left[P_a(t)(1-P_{u21}(t))+(1-P_{u1}(t))(1-P_{u22}(t))\right]\times$$

$$\times P_{u32}(t)P_{u42}(t),$$

$$P_6(t) = P_a(t)(1-P_{u1}(t))P_{u22}(t).$$

Таким образом, вероятность преодоления системы контроля доступа и получения несанкционированного доступа к ресурсам сети связи общего пользования можно определить как:

$$P_{НСД} = 1 - \sum_{i=1}^{6} P_i(t).$$

Основные сложности использования аналитических зависимостей вычисления базовых показателей предотвращения несанкционированного доступа к ресурсам сети связи общего пользования средствами контроля доступа заключаются в формировании исходных данных для расчета, которые могут быть получены как на основе долговременного сбора статистической информации и ее последующей обработки, так и методами испытаний. Однако, несмотря на все сложности, рассмотренная математическая модель позволяет со значительной степенью достоверности формализовать процесс функционирования системы контроля доступа.

ВЫВОДЫ

Таким образом, рассмотренные методы обоснования требований к системе обеспечений безопасности информации позволяют в общих чертах определить характеристики структуры проектируемой системы защиты и применяемых методов обеспечения безопасности информации, однако не позволяют обосновать значения

количественных характеристик разрабатываемых систем. Этот недостаток отсутствует при использовании методов на основе анализа степени риска и вероятностной модели.

Анализ современных методов обоснования требований к системам защиты позволяет сделать вывод, что наиболее эффективным является метод на основе вероятностной модели исходов.

Основные сложности использования аналитических зависимостей вычисления базовых показателей предотвращения несанкционированного доступа к ресурсам сети связи общего пользования средствами контроля доступа заключаются в формировании исходных данных для расчета, которые могут быть получены как на основе долговременного сбора статистической информации и ее последующей обработки, так и методами испытаний. Однако, несмотря на все сложности, рассмотренная математическая модель позволяет со значительной степенью достоверности формализовать процесс функционирования системы контроля доступа.

СПИСОК ЛИТЕРАТУРЫ

1. Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации: Сборник руководящих документов по защите от НСД. М.: Гостехкомиссия России, 1998. С. 23–52.

2. **Попов О. В.** Некоторые вопросы защиты банковской конфиденциальной информации // Безопасность информационных технологий. 1995. № 1 . С. 53–61.

3. **Герасименко В. А.** Защита информации в АСОД. М.: Энергоатомиздат, 1994.

4. **Герасименко В. А.** Основы теории управления качеством информации // Деп. ВИНИТИ, № 5392-В89.1989.

5. **Ухлимов Л. М., Казарин О. В.** Методология защиты информации в условиях конверсии военного производства // Вестник ВОИВТ. 1994. № 1–2. С. 55–60.

ОБ АВТОРАХ

Виноградова Ирина Леонидовна, преп. каф. телекоммуникац. систем, лектор Ин-та инфокоммуникац. технологий. Дипл. инженер по инф.-измерительн. системам (УГАТУ, 1992). Д-р техн. наук. Иссл. в обл. оптики, волоконно-оптической связи, теории обработки сигналов.

Даннави Мохамад Насреддин, асп. Дипл. инженер по многоканальной связи (МТУСИ, 2006). Иссл. в обл. информац. безопасности, волоконно-оптическ. связи, сетей нового поколения.