С. В. Скрыль, А. П. Курило, В. Н. Финько, В. Н. Чашкин

КОНФИДЕНЦИАЛЬНОСТЬ КАК СУБЪЕКТИВНЫЙ ПОКАЗАТЕЛЬ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

Степень обеспечения защищенности информации определяется качеством защиты информации, т. е. совокупностью свойств и характеристик такого рода деятельности как информационной услуги, придающих ей способность соответствовать установленным или возможным требованиям. Вместе с тем при обеспечении защищенности информации в конкретных условиях возникает ряд трудностей, связанных с отсутствием как перечня ее свойств и характеристик, так и области допустимых их значений. Это приводит к необходимости ограничиться пониманием следующих аспектов проблемы обеспечения защищенности информации:

1. Защищенность информации является обобщенной характеристикой состояния информации, при котором на заданном уровне осуществляется поддержание установленного статуса ее хранения, обработки и использования.

2. Требуемый и реально предоставляемый уровни защищенности информации определяются соответственно потребностями в поддержании установленного статуса хранения, обработки и использования информации и применяемыми технологиями ее защиты.

3. Требуемый и предоставляемый уровни обеспечения защищенности информации есть функции времени.

Обоснованный выбор требуемого уровня защищенности информации является крайне сложной проблемой, поэтому целесообразно исходить из посылки, что такой уровень может быть адекватно оценен лишь степенью достижения целей защиты информации. Естественно, что целью деятельности по защите информации является установленный статус ее хранения, обработки и использования. Из этого следует, что, во-первых, понятие защищенности информации обладает определенным набором свойств и характеристик статуса ее хранения, обработки и использования и, во-вторых, такой набор свойств и характеристик должен быть оцениваемым.

Вместе с тем неоднозначность самого понятия «информация» [1], многообразие ее свойств, сложность и организационная природа деятельности по защите информации, широкий диапазон и динамика пользовательских требований к такого рода деятельности привели к появлению значительного и варьируемого количества различных, слабо связанных или не связанных между собой показателей, характеризующих:

объективные свойства обеспечения защищенности информации, являющиеся инвариантами для условий деятельности по защите информации, архитектуры систем защиты информации и используемым технологиям защиты

и субъективные свойства обеспечения защищенности информации — способность подобного рода деятельности как информационной услуги отвечать определенным пользовательским требованиям.

Это приводит к необходимости поиска показателя, сочетающего в себе как объективные, так и субъективные свойства. С этой целью дадим характеристику этим свойствам.

К объективным показателям защищенности информации можно отнести [1–3]:

- объем защищаемой информации ($d_1^{(o)}$), характеризующий потребности в обеспечении установленного статуса ее хранения, обработки и использования;
- время выполнения процедуры защиты ($d_2^{(o)}$), характеризующее временной интервал с момента начала действий, предпринятых для выполнения процедуры защиты информации, до момента их завершения.

Вместе с тем использование объективных показателей для характеристики всех свойств защищаемой информации как продукта информационной деятельности сопряжено с рядом трудностей, обусловленных следующими обстоятельствами. Современное состояние информатики как науки позволяет с помощью объективных показателей описать и измерить с той или иной степенью точности различные свойства информации и как информационной сущности, обладающей определенной семантикой, и как предмета информационной технологии и технологии ее защиты, реализуемой с использованием конкретного ресурса. Однако при этом может существовать ряд обстоятельств, значительно ограничивающих их применение. К ним относятся:

1) отсутствие возможности использования объективных методов измерения;

2) существование у неподготовленного пользователя интуитивной и естественной трудности конкретного восприятия достаточно абстрактных объективных показателей;

3) свойство услуги, воспринимаемое пользователем, интегрирует в себе ряд свойств и может быть корректно описано лишь в виде вектора, в то время как объективные показатели являются показателями скалярного типа;

4) специфичность процессов противодействия угрозам информационной безопасности, качество обеспечения которых оценивается предотвращенным ущербом и носит ярко выраженный субъективный характер [4].

Психофизиологическое преодоление названных трудностей определяет существование субъективных показателей защищенности информации, зависящих от реакции пользователя на объективные показатели.

Несмотря на различную природу объективных и субъективных показателей защищенности информации, их мера имеет общие признаки:

— нетривиальную определимость (трудности формулирования и формального описания) и количественную оценку;

— нечеткость измерения;

— неоднозначную, неформализуемую взаимосвязь;

— отсутствие инвариантности (зависимость значения показателя от конкретного вида информационной деятельности и ее условий);

— возможную альтернативность показателей;

— широкий доверительный интервал вычислительной оценки и др.

Являясь производными от объективных показателей защищенности информации, субъективные показатели характеризуют технологию защиты в части возможностей по поддержанию установленного статуса хранения, обработки и использования информации. Область оценки по каждому показателю детерминирована субъектом деятельности в соответствии со степенью удовлетворенности его потребностей при применении той или иной технологии защиты информации. Иными словами, подобного рода показатели отражают способность информации сохранять установленный статус хранения, обработки и использования. К субъективным показателям качества защиты информации относятся [5—7]:

- конфиденциальность информации ($d_1^{(c)}$), характеризующая требование, обязательное для выполнения лицом, получившим доступ к определенной информации, не передавать такую информацию третьим лицам без согласия ее обладателя;

- целостность информации ($d_2^{(c)}$), характеризующая способность обеспечивать предоставление права ее модификации (уничтожения) только в соответствии с правилами разграничения доступа, а также обеспечивать неизменность в условиях случайных ошибок или стихийных бедствий;

- доступность информации ($d_3^{(c)}$), характеризующая способность обеспечивать свободный доступ к ней по мере возникновения необходимости (в [6] — возможность получения информации и ее использования);

- своевременность реализации функций защиты информации ($d_4^{(с)}$), характеризующая время, в течение которого эти функции удовлетворяют предыдущие требования.

По сути, конфиденциальность является нормированным показателем допустимого уровня защищенности информации. Формально можно считать, что

$d_1^{(с)} = 1$ при $d_1^{(о)} \ \upsilon_{(д)}$ (1)

и $d_1^{(с)} = 0$ при $d_1^{(о)} > \upsilon_{(д)}$, (2)

где $\upsilon_{(д)}$ — максимально допустимый для данных условий объем информации, для которой может быть обеспечен установленный статус хранения, обработки и использования.

Будем полагать, что условие (1) является обязательным требованием к реализации процедур защиты информации. В противном случае (условие (2)) процедура защиты информации не реализуется.

Исходя из изложенного фундаментальным и наиболее общим и употребительным показателем защищенности информации является обеспечение ее конфиденциальности в условиях своевременной реализации функций защиты информации при заданных уровнях ее целостности и доступности. В конечном итоге именно этот показатель определяет удовлетворение или неудовлетворение потребностей в защите информации.

В качестве доказательства о функциональной зависимости как объективных, так и субъективных показателей деятельности по защите информации от ее конфиденциальности оценим условно верхний уровень любого из рассмотренных показателей единицей. Тогда можно полагать, что

$d_i^{(о)} \to 1$, $i = 1, 2$, $d_j^{(с)} \to 1$, $j = 2, 3, 4$, при $d_1^{(с)} \to 1$.

Такие допущения позволяют производить оценку защищенности информации посредством измерения необходимого уровня обеспечения конфиденциальности при заданных уровнях ее целостности, доступности и своевременности реализации процедур защиты.

Это позволяет при реализации одного из основополагающих принципов решения ряда задач обоснования требований к способам и средствам защиты информации — принципа однородности представления характеристик процессов защиты информации — использовать в качестве основания для унификации описания соответствующих механизмов объем защищаемой информации. Кроме того, эти параметры позволяет дать количественное представление эффективности этих процессов [8].

Следует отметить, что в проблематике обеспечения информационной безопасности при организации защиты информации рассмотренные обстоятельства являются определяющими. Кроме того, из анализа условий (1) и (2) становится очевидным следующее:

1) максимально допустимый для данных условий объем информации, для которой может быть обеспечен установленный статус хранения, обработки и использования, можно рассматривать как один из параметров, характеризующих функционал ущерба, который может понести информационная деятельность вследствие угрозы информационной безопасности;

2) условие (1) является обязательным требованием к реализации процедур защиты информации;

3) в противном случае (условие (2)) реализация процедур защиты информации теряет всякий смысл;

4) показатель конфиденциальности информации носит вероятностный характер [8]:

$0 \le d_1^{(с)} \le 1$.

В совокупности указанные предпосылки создают основу научно-методологической базы для исследования вопросов обеспечения защищенности информации.

СПИСОК ЛИТЕРАТУРЫ:

1. *Минаев В. А., Скрыль С. В., Дворянкин С. В. и др.* Информатика: учебник для высших учебных заведений МВД России. Том 1. Информатика: Концептуальные основы. М.: Маросейка, 2008. — 464 с.
2. Основы информационной безопасности: учебник для высших учебных заведений МВД России / Под ред. В. А. Минаева и С. В. Скрыля. Воронеж: Воронежский институт МВД России, 2001. — 464 с.
3. *Гаранин М. В., Новокшанов И. В., Скрыль С. В. и др.* Информационная безопасность телекоммуникационных систем (технические вопросы): учебное пособие для системы высшего профессионального образования России. М.: Радио и связь, 2004. — 388 с.
4. *Скрыль С. В., Багаев Д. А.* Своевременность как базовый показатель качества защиты информации // Вопросы защиты информации. 2009. № 2. С. 61— 63.
5. *Герасименко В. А., Малюк А. А.* Основы защиты информации: учебник для высших учебных заведений Министерства общего и профессионального образования РФ. М.: МИФИ, 1997. — 538 с.
6. Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149—ФЗ // Российская газета. 2006. 29 июля.
7. *Минаев В. А., Скрыль С. В., Дворянкин С. В. и др.* Правовое обеспечение информационной безопасности: учебник для высших учебных заведений МВД России. М.: Маросейка, 2008. — 368 с.
8. *Петренко П. Б., Джоган В. К., Ромендик Р. В.* Функция-модель механизмов защиты информации в компьютерных системах объектов промышленно-деловой среды // Вопросы защиты информации. 2009. № 2. С. 49—51.