*М. М. Коптенков*

# КАТЕГОРИРОВАНИЕ ИНФОРМАЦИИ – ПЕРВЫЙ ШАГ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Информационная безопасность — это состояние защищенности информационной среды. Информационная безопасность должна рассматриваться как комплекс мер, среди которых нельзя выделить более или менее важные [1]. Понятие информационной безопасности тесно связано с понятием защиты информации, которое представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на нее, т. е. процесс, направленный на достижение состояния информационной безопасности. Однако прежде чем защищать информацию, необходимо определить, какую именно информацию следует защищать и в какой степени. Для этого применяется *категорирование* (классификация) информации, т. е. установление градаций важности обеспечения безопасности информации и отнесение конкретных информационных ресурсов к соответствующим категориям. Таким образом, категорирование информации можно назвать первым шагом на пути к обеспечению информационной безопасности организации.

Исторически сложилось, что при классификации информации ее сразу же начинают классифицировать по уровню секретности (конфиденциальности). При этом требования по обеспечению доступности и целостности часто не учитываются или учитываются наравне с общими требованиями к системам обработки информации. Это неверный подход. Во многих областях доля конфиденциальной информации сравнительно мала. Для открытой информации, ущерб от разглашения которой отсутствует, важнейшими свойствами являются: доступность, целостность и защищенность от неправомерного копирования [2–3]. В качестве примера можно привести интернет-магазин, где важно постоянно поддерживать доступность к веб-сайту компании.

Исходя из необходимости обеспечения различных уровней защиты информации можно ввести различные категории конфиденциальности, целостности и доступности.

## 1. Категории конфиденциальности защищаемой информации

Конфиденциальность информации — свойство информации, указывающее на необходимость введения ограничений на круг лиц, имеющих доступ к данной информации [2]. Вводятся следующие категории конфиденциальности информации:

— *Строго конфиденциальная информация* — информация, являющаяся конфиденциальной в соответствии с требованиями законодательства, а также информация, ограничения на распространение которой введены решениями руководства организации, разглашение которой может привести к нанесению значительного ущерба деятельности организации.

— *Конфиденциальная информация* — информация, не являющаяся строго конфиденциальной, ограничения на распространение которой вводятся только решением руководства организации, разглашение которой может привести к нанесению ущерба деятельности организации.

— *Открытая информация* — к данной категории относится информация, обеспечения конфиденциальности которой не требуется.

## 2. Категории целостности информации

Целостность информации — свойство, при выполнении которого данные сохраняют заранее определенный вид и качество (остаются неизменными по отношению к некоторому фиксированному состоянию).

Вводятся следующие категории целостности информации:

— *Высокая* — к данной категории относится информация, несанкционированная модификация или подделка которой может привести к нанесению значительного ущерба деятельности организации.

— *Низкая* — к данной категории относится информация, несанкционированная модификация которой может привести к нанесению умеренного или незначительного ущерба деятельности организации.

— *Нет требований* — к данной категории относится информация, к обеспечению целостности которой требований не предъявляется.

### 3. Категории доступности информации

Доступность — состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно [2].

Вводятся следующие категории доступности информации:

— *Беспрепятственная доступность* — доступ к информации должен обеспечиваться в любое время (задержка получения доступа к информации не должна превышать нескольких секунд или минут).

— *Высокая доступность* — доступ к информации должен осуществляться без существенных временных задержек (задержка получения доступа к информации не должна превышать нескольких часов).

— *Средняя доступность* — доступ к информации может обеспечиваться с существенными временными задержками (задержка получения информации не должна превышать нескольких дней).

— *Низкая доступность* — временные задержки при доступе к информации практически не лимитированы (допустимая задержка получения доступа к информации — несколько недель).

Из вышеперечисленного видно, что категории конфиденциальности и целостности информации напрямую зависят от величины ущерба деятельности организации при нарушении этих свойств информации. Категории доступности в меньшей степени, но также зависят от величины ущерба деятельности организации. Для определения величины ущерба используется его субъективная оценка и вводится трехуровневая шкала: значительный ущерб, умеренный ущерб и низкий ущерб (или отсутствие ущерба).

Ущерб деятельности организации оценивается как *низкий*, если потеря доступности, конфиденциальности и/или целостности информации оказывает незначительное негативное воздействие на деятельность организации, ее активы и персонал. Незначительность негативного воздействия означает, что:

- организация остается способной выполнять свою деятельность, но эффективность основных функций оказывается сниженной;
- активам организации наносится незначительный ущерб;
- организация несет незначительные финансовые потери.

Ущерб деятельности организации оценивается как *умеренный*, если потеря доступности, конфиденциальности и/или целостности оказывает серьезное негативное воздействие на деятельность организации, ее активы и персонал. Серьезность негативного воздействия означает, что:

- организация остается способной выполнять свою деятельность, но эффективность основных функций оказывается существенно сниженной;
- активам организации причиняется значительный ущерб;
- компания несет значительные финансовые потери.

Потенциальный ущерб для организации оценивается как *значительный*, если потеря доступности, конфиденциальности и/или целостности оказывает тяжелое (катастрофическое) негативное воздействие на деятельность организации, ее активы и персонал, т. е.:

- организация теряет способность выполнять все или некоторые из своих основных функций;
- активам организации причиняется крупный ущерб;
- организация несет крупные финансовые потери.

Таким образом, оценивая ущерб деятельности организации при нарушении конфиденциальности, целостности и доступности информации и на основании этого определяя категории информации, можно выделить три ее типа: наиболее критичная, критичная и некритичная.

Определение типа информации осуществляется путем сопоставления категорий этой информации. В таблице 1 приведено определение типа информации.

*Таблица 1. Определение типа информации*

| **Категория конфиденциальности информации** | **Категория целостности информации** | **Категория доступности информации** | **Тип информации** |
|---|---|---|---|
| Строго конфиденциальная информация | * | * | Наиболее критичная информация |
| * | Высокая | * | |
| * | * | Беспрепятственная доступность | |
| Конфиденциальная информация | * | * | Критичная информация |
| * | Низкая | * | |
| * | * | Высокая доступность | |
| Открытая информация | Нет требований | Средняя доступность | Некритичная информация |
| Открытая информация | Нет требований | Низкая доступность | |

Таким образом, категорирование информации является первым шагом к обеспечению информационной безопасности организации, так как, прежде чем что-то защищать, в первую очередь, стоит определить, что именно требуется защищать и в какой степени. Категорировать следует и пользовательскую, и системную информацию, представленную как в электронной форме, так и на материальном носителе. Для определения типа защищаемой информации необходимо определить, какой ущерб организации будет причинен при потере конфиденциальности, целостности и доступности такой информации.

В дальнейшем, определив, к какому типу какая информация относится, можно применять различные меры по защите каждого типа информации. Это позволит не только структурировать обрабатываемые в организации данные, но и наиболее эффективно внедрить и использовать подсистему управления доступом к защищаемой информации, а также оптимизировать затраты на обеспечение информационной безопасности.

## СПИСОК ЛИТЕРАТУРЫ:

1. *Безмалый В.* Служба защиты информации: первые шаги. 2008 г. URL: http://www.compress.ru/Article.aspx?id=20512.
2. Категорирование информационных ресурсов. URL: http://inf-bez.ru/?p=152.
3. *Гладких А. А., Дементьев В. Е.* Базовые принципы информационной безопасности вычислительных сетей. Ульяновск: УлГТУ, 2009. – 156 с.