EUROLAB “Cook Book” – Doc No. 21
Translated into Russian by LLC “Profilab” (with the permission of EUROLAB)

“Поваренная книга” EUROLAB – Документ No. 21
Переведено на русский язык ООО “Профилаб” (с разрешения EUROLAB)

Классификация и обработка информации в лаборатории

ВВЕДЕНИЕ

Лаборатория обрабатывает много видов информации. Существуют некоторые требования к обработке информации лабораторией. Требования могут быть законодательными, устанавливаться стандартами, заказчиками и аккредитацией. Чтобы иметь возможность отвечать этим требованиям, лаборатория должна иметь систему управления информацией. Однако намного более эффективной обработку информации сделает также модель классификации.

ТРЕБОВАНИЯ

Настоящая кулинарная книга и модель классификации информации основаны на модели MSB:s (Агентство по чрезвычайным ситуациям Швеции) [1], RISE (Исследовательские институты Швеции) разработали модель MSB [2], которая основана на серии стандартов ISO/IEC 27000 [3-5]. В ISO/IEC 17025:2017 [6] установлены некоторые требования, касающиеся обработки информации, например, пп. 4.2.1, 7.11.1 и 7.11.2. В дополнение, особенно п. 7.11.3, установлены требования к самой системе управления информацией с точки зрения защиты данных и условий окружающей среды для работы, а также техническому обслуживанию для обеспечения целостности данных и обработки информации. Классификация может помочь выполнить эти требования.

Также существуют специальные стандарты по информационной безопасности, например, серия стандартов ISO/IEC 27000 [3-5].

ЖИЗНЕННЫЙ ЦИКЛ ИНФОРМАЦИИ

Информация имеет жизненный цикл (см. ниже). Изначально классификацию информации следует выполнять в связи с созданием. Однако в течение «жизни» информации классификация может измениться из-за обработки и модификации информации или просто из-за того, что прошло время.

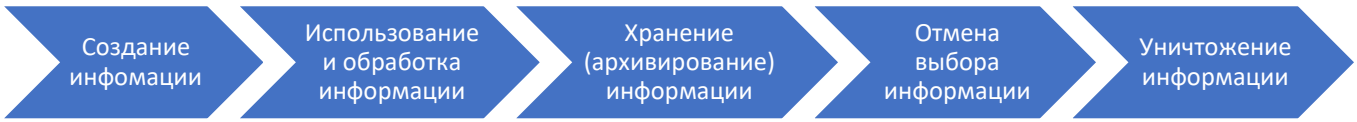

Рисунок 1. Жизненный цикл информации

МОДЕЛЬ ДЛЯ КЛАССИФИКАЦИИ ИНФОРМАЦИИ

Классификация информации может помочь обеспечить правильный уровень защиты информации. Ее классификация зависит от ее назначения и важности для организации. Модель классификации информации/вида информации основана на последствиях, которые могут вызвать нежелательные влияния на качество информации. Последствия оцениваются с точки зрения влияния на организацию.

Аспекты безопасности

В модели используются следующие аспекты безопасности:

- Конфиденциальность: насколько открыта (*прим. пер.* – для доступа) информация? Открыта для всех? или держится в секрете?
- Точность: информация должна быть надежной, корректной и полной и не должна быть изменена или искажена ни в результате неправильного понимания, ни в результате функциональной ошибке, ни в результате несанкционированного обращения (*прим. пер.* – с информацией).
- Доступность: информация должна быть предоставлена организацией соответствующему персоналу с надлежащим доступом в течение согласованного периода.
- Прослеживаемость: любая деятельность, выполняемая с информацией, должна быть прослеживаема, и должно быть ясно, кто такую деятельность выполнил.

Уровни последствий

Последствия потери конфиденциальности, точности, доступности и прослеживаемости (*прим. пер.* – информации) для организации, других организаций или отдельных лиц можно классифицировать как:

- отсутствие ущерба или незначительный ущерб;
- умеренный ущерб;
- существенный ущерб;
- опасный ущерб;
- катастрофический ущерб.

Уровни аспектов безопасности

На основании вышеизложенного рассмотрения каждый из аспектов безопасности можно классифицировать по различным уровням последствий: например, от 0 (требуется низкий уровень безопасности) до 4 (требуется высокий уровень безопасности).

Например, когда речь идет о конфиденциальности (см. также пример ниже), ее можно классифицировать как:

- открытая информация (уровень 0);
- внутренняя (внутри организации) информация (уровень 1);
- ограниченная внутренняя информация (уровень 2);
- секретная информация (уровень 3);
- секретная информация, касающаяся компетентности (уровень 4).

Классификация и обработка

Для вычисления окончательной классификации можно использовать различные инструменты. Первый и самый очевидный инструмент – это электронная таблица, например, Excel. Можно использовать алгоритмы, чтобы свести различные аспекты безопасности и уровни последствий в одну цифру.

Поскольку довольно сложно учесть все аспекты безопасности, можно сосредоточиться на одном или двух аспектах, обычно конфиденциальность является одним из них, и провести классификацию информации.

Также необходимо провести классификацию систем, в которых обрабатывается классифицированная информация, например, различные IT-системы, архивы, помещения и т. д. Это выполняется почти таким же способом, как и классификация информации. После проведения классификации информации/вида информации, организация может принять решение об уровне необходимой защиты: кто, как и где будет обрабатывать определенный вид информации (например, не разрешается обрабатывать информацию, которая была классифицирована как секретная в открытой IT-системе).

Уровень необходимой защиты

Общая оценка аспектов безопасности и последствий приводит к установлению требований к уровню защиты информации и к системам (IT или другим), которые используются для ее обработки и архивирования. Это включает требования к:

- сроку хранения;
- носителю для архивирования;
- локализации архива;
- поддержке и уровню обслуживания.

Ссылки

[1] Modell för klassificering av information, Version 1.0, 2009-05-25, Publikationsnummer: MSB 0040-09 (*Модель для классификации информации*)

[2] M. Antonsson**,** Riktlinjer för informationsklassning, 2018-11-09, RISE 19366 Version 1.0 (*Рекомендации по классификации информации*)

[3] ISO/IEC 27000:2018 – Information technology – Security techniques – Information security management systems – Overview and vocabulary
(ISO/IEC 27000:2018 *Информационные технологии – Методы обеспечения безопасности – Системы менеджмента информационной безопасности – Общий обзор и словарь*)

[4] ISO/IEC 27001:2013[1] – Information technology – Security techniques – Information security management systems – Requirements
(ISO/IEC 27001:2013 *Информационные технологии – Методы обеспечения безопасности – Системы менеджмента информационной безопасности – Требования*)

[5] ISO/IEC 27002:2013[2] – Information technology – Security techniques – Code of practice for information security controls
(ISO/IEC 27002:2013 *Информационные технологии – Методы обеспечения безопасности – Кодекс практики для средств управления информационной безопасностью*)

[6] ISO/IEC 17025:2017 General requirements for the competence of testing and calibration laboratories
(ISO/IEC 17025:2017 *Общие требования к компетентности испытательных и калибровочных лабораторий*)

[1] Заменен на ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements (*Информационная безопасность, кибербезопасность и защита конфиденциальности – Системы менеджмента информационной безопасности – Требования*)
[2] Заменен на ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls (*Информационная безопасность, кибербезопасность и защита конфиденциальности – Управление информационной безопасностью*)

Пример

Пример классификации аспекта безопасности «конфиденциальность». Это следует делать для каждого вида информации (или системы информации):

- оцените аспект безопасности, следуя схеме на рисунке 2, для каждого шага в его жизненном цикле;
- заполните таблицу 1.

Выполните такую же оценку для других аспектов безопасности: точности, доступности и прослеживаемости. Основываясь на полученных оценках решите, к какому уровню безопасности будет отнесена эта информация. Обратите внимание, что уровень безопасности может меняться на протяжении жизненного цикла. В этом случае обычно выбирается самый высокий уровень в качестве конечного уровня.

Основываясь на конечном уровне и типе информации, вы можете принять решение об уровне необходимой защиты, как упомянуто выше.

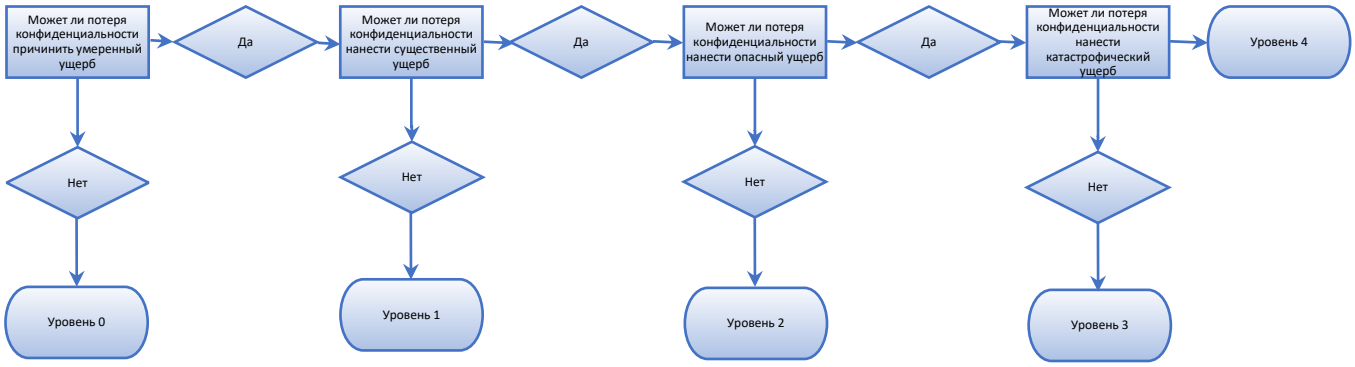

Рисунок 2.

Аспект безопасности	Жизненный цикл	Уровни последствий	Мотивация	Комментарии
Конфиденциальность	Создание	1		
Конфиденциальность	Использование и обработка	2		
Конфиденциальность	Хранение	3		
Конфиденциальность	Отмена выбора	3		
Конфиденциальность	Уничтожение	0		
Конфиденциальность	Общий вывод			

Таблица 1. Таблица для классификации информации

За перевод настоящей CookBook и любые дополнительные правки несет ответственность ООО «Профилаб».