**Аннотация доклада Трубея А.И.**

**«Оценка рисков информационной безопасности»**

**(29.11.2016)**

Достижение требуемого уровня ИБ в любой организации должно базироваться на исследовании источников угроз информации, уязвимостей в ее защите, и проистекающих из их соотношений рисков. Механизм эффективного противодействия угрозам ИБ содержится в доступных международных стандартах, прежде всего в современных риск-ориентированных стандартах ISO (International Organization for Standardization) и аналогичных национальных стандартах.

Оценка рисков ИБ и их периодическая переоценка является неотъемлемой частью создания и функционирования системы менеджмента информационной безопасности (СМИБ), разрабатываемой с целью выбора адекватных и соразмерных средств управления безопасностью, которые предназначены для защиты информационных активов и придают уверенность заинтересованным сторонам. Это положение закреплено в СТБ ISO/IEC 27001-2011 и в других нормативных документах. Наиболее подходящим для большинства практических применений является определение риска ИБ, приведенное в стандарте СТБ ISO/IEC 27005-2012. Согласно СТБ ISO/IEC 27005-2012 риск ИБ – это потенциальная возможность использования уязвимостей актива или группы активов конкретной угрозой для причинения ущерба организации. Стандарт конкретизирует понятие риска ИБ, раскладывая его на активы, угрозы, уязвимости и ущерб и предлагает процесс менеджмента рисков ИБ, включающий несколько последовательных шагов (идентификация, анализ, оценка, обработка и т. д.) и две критические точки принятия решения: обрабатывать ли конкретный риск и считается ли данный риск приемлемым.

1. В докладе приводится расчет риска ИБ по методике GlobalTrust. Методика характеризуется следующими особенностями:

- риск оценивается для конкретных активов или групп активов;

- риск определяется качественно и количественно на основании трех параметров: вероятности угрозы, величины уязвимости, размера ущерба;

- для оценки риска используется многоуровневая качественная шкала;

Для вычисления рисков используется период времени, равный одному году. В этом случае величина риска соответствует прогнозируемым среднегодовым потерям в результате инцидентов безопасности  (Annual Loss Expectancy). Величина риска  определяется по формуле: 

где:  (Asset Value) – стоимость подвергаемых риску активов системы (данных, программ, аппаратуры и т.д.);

 (Exposure Factor) – степень уязвимости актива к угрозе;

 (Annualized Rate of Occurrence) – среднегодовая частота возникновения инцидентов, величина, представляющая собой ожидаемую частоту реализации угрозы в год.

2 Оценка уязвимостей, связанных с дефектами и ошибками ПО, при проектировании или кодировании осуществляется с использованием Системы оценки общеизвестных уязвимостей (Common Vulnerability Scoring System – CVSS). Она состоит из 3 групп метрик: базовые метрики, временные метрики и контекстные метрики. Каждая метрика представляет собой число (оценку) в интервале 0 – 10 и вектор – краткое текстовое описание со значениями, которые используются для вывода оценки.

3. Оценка уровня опасности уязвимости осуществляется по шкале [FortiGuard](http://www.fortiguard.com/static/intrusion/severity.html).

|  |  |
| --- | --- |
| Уровень опасности FortiGuard | Оценка по CVSS 2.0 |
| Критический | 9 – 10 |
| Высокий | 7 – 8.9 |
| Средний | 4 – 6.9 |
| Низкий | 0.1 – 3.9 |
| Информационный | 0 |

4 Для оценки рисков используется банк данных угроз безопасности информации ФСТЭК России и Словарь общеизвестных уязвимостей, который имеет строгую характеристику по описательным критериям (Common Vulnerabilities and Exposures – CVE).

5 Для оценки возможного ущерба могут использоваться различные критерии и качественные шкалы. Для того, чтобы оценка ущерба имела экономический смысл, качественная шкала должна соотноситься с размером финансовых потерь. Размер ущерба, как правило, выражается в денежных единицах.

Например, в качестве информационных активов, в отношении которых осуществляются угрозы информационной безопасности, можно рассматривать геологические, геофизические, геохимические и иные данные, характеризующие особенности строения и минерально-сырьевой потенциал недр, зафиксированные на материальных носителях, накопленные и обрабатываемые с использованием ИС.

Хищение данных может привести к нарушению их конфиденциальности и прав собственности. Сведения могут быть использованы физическими или юридическими лицами, которые не предусмотрены в государственных контрактах или других соглашениях (лицензиях, договорах) на производство работ по геологическому изучению недр. В результате, возможно, придется уплачивать штрафы по искам клиентов на основании заключенных с ними соглашений о конфиденциальности. Кроме того, будет нанесен ощутимый урон репутации, который выльется в сокращении числа клиентов, заказов и уменьшении коммерческой выручки. Выход из строя информационной системы (нарушение доступности информации) может привести к срыву выполнения бизнес-планов, проектов, договорных обязательств.

6. Для оценки риска можно использовать качественную шкалу, в которой определенным уровням риска сопоставляются соответствующие размеры среднегодовых потерь. В основу оценки ущерба может быть положен подход, применяемый в Уголовном кодексе (УК) Республики Беларусь (глава 24).

|  |  |
| --- | --- |
| Уровень ущерба (риска) | Среднегодовой ущерб в результате инцидентов безопасности – ALE (базовых величин**\***) |
| Незначительный |  0 ≤ ALE < 40 базовых величин  |
| Значительный | 40 базовых величин ≤ ALE < 250 базовых величин |
| Крупный | 250 базовых величин ≤ ALE < 1000 базовых величин |
| Особо крупный |  1000 базовых величин ≤ ALE  |
| Примечание – базовая величина с 01.01.2016 составляет 21. белорусский рубль |