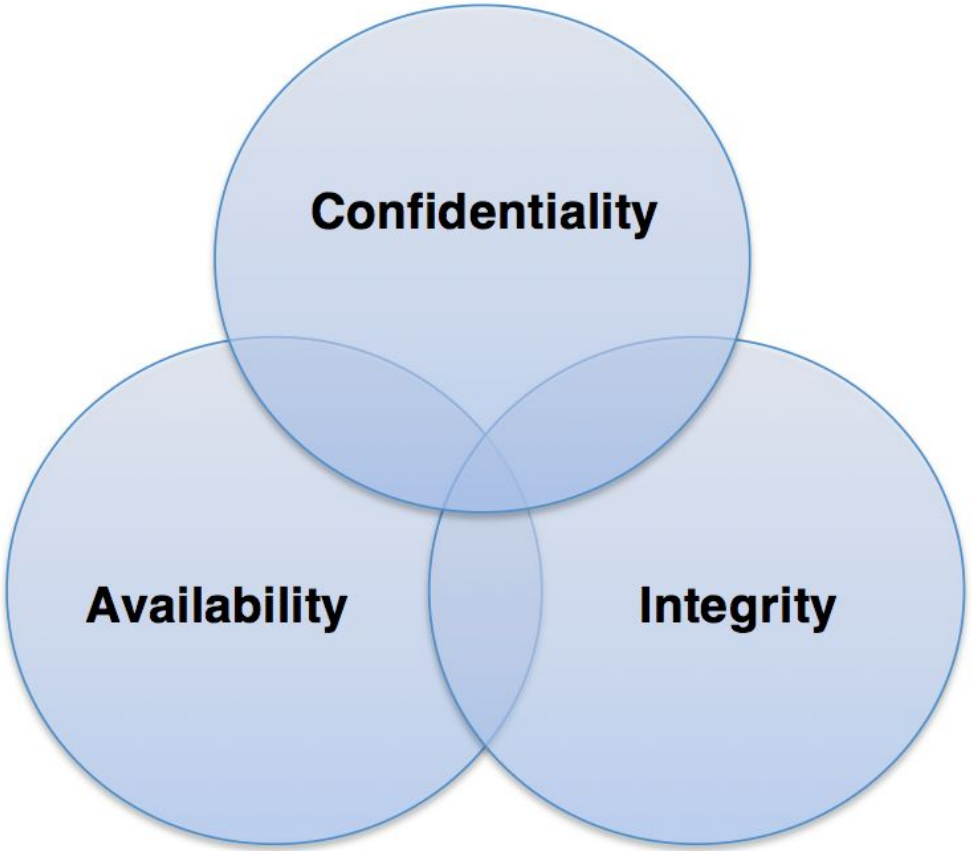
Методика оценки критичности информации

Классификация (категоризация) информационных систем.

Методика устанавливает уровень критичности информационных систем. Уровень критичности определяется потенциальным ущербом для организации, в отношении которой производятся действия, ставящие под угрозу безопасность информации и информационных систем, необходимых организации для достижения поставленных задач, защиты ее активов, выполнения своих правовых обязанностей, поддержания на должном уровне своих ежедневых функций и защиты людей. Категоризация безопасности должна также рассматривать информацию о уязвимости и угрозах, соответствующих информационной системе.

Атрибуты безопасности

Общепринято, что информационная безопасность ни что иное, как сохранение трех нижеприведённых атрибутов безопасности. Все негативные воздействия на систему безопасности, в основном, связаны с нарушением одного или нескольких из этих атрибутов.



1. Конфиденциальность (Confidentiality)

«Сохранение авторизированных ограничений на раскрытие и доступ к информации, включая средства защиты неприкосновенности личной жизни и служебной (патентной) информации…»

Потеря конфиденциальности является несанкционированным раскрытием информации.

2. Целостность (Integrity)

«Охрана информации от ее не надлежащей модификации или уничтожения включает в себя обеспечение безоговорочности и правдивости информации…»

Потеря целостности это не авторизированное изменение или разрушение информации.

3. Доступность (Availability)

«Обеспечение своевременного и надежного доступа к информации и к ее использованию…»

Потеря доступности это нарушение доступа к информации и к ее использованию, также к информационной системе.

Потенциальный ущерб

Все информационные системы могут быть подразделены на системы с НИЗКИМ, СРЕДНИМ и ВЫСОКИМ уровнем потенциального ущерба, в зависимости от оценочного ущерба.

НИЗКИЙ потенциальный ущерб

Ожидается, что потеря конфиденциальности, целостности и доступности будет иметь ограниченное воздействие на организацию[1] и на физических лиц[2].

СРЕДНИЙ потенциальный ущерб

Ожидается, что потеря конфиденциальности, целостности и доступности будет иметь серьезное негативное влияние на организацию и физических лиц.

ВЫСОКИЙ потенциальный ущерб

Ожидается, что потеря конфиденциальности, целостности и доступности будет иметь тяжелое или катастрофически негативное влияние на организацию и физических лиц.

---

[1] Организация или Государственный орган, владеющий информационной системой.

[2] Физические лица, являющиеся персоналом, использующим или связанным с информационной системой.

Метод категоризации безопасности информационных систем

Для информационной системы, значение потенциального ущерба может быть определено путем оценки организации и индивидуальных ущербов, соответствующих нарушению атрибутов безопасности (Конфиденциальность, Целостность и Доступность). Совокупный ущерб для информационной системы является функцией различных ущербов

1. Ущерб организации (Материальный)

Ущерб организации, влекущий прямые финансовые потери, вызван рисками или слабыми сторонами системы. Такой ущерб может быть оценен количественно.

1.1 Стоимость поврежденных активов

Финансовый ущерб, вызванный потерей или повреждением активов, таких как аппаратные средства, программное обеспечение и другая инфраструктура.

1.2 Стоимость восстановления

Финансовые потери, вызванные необходимыми затратами на ремонт оборудования, восстановления программного обеспечения или информации и восстановление оказания услуг. Они включают в себя затраты на выявление, устранение и восстановление и возобновления операций для каждой системы.

1.3 Потеря доходов

Финансовый ущерб, вызванный перебоями в системах, генерирующих доход.

2. Ущерб организации (Не материальный)

Ущерб организации, влекущий непрямые финансовые потери, вызван рисками или слабыми сторонами системы. Такие виды ущерба не могут быть измерены количественно, однако могут быть оценены качественно, как ‘высокий‘,‘средний ‘,‘низкий‘ и тд.

2.1 Потеря/ухудшение функциональности

Ущерб вызван потерями/ухудшением функциональности или вмешательствами в услуги, предоставляемые системой. Также недостаточной проработкой целей и задач.

2.2 Потеря имиджа/репутации

Ущерб, нанесен утратой доверия пользователя, потери доброжелательности/негативного воздействия на репутацию, ослабление способности к переговорам, потери конкурентных преимуществ, потеря доверия, потеря технической репутации и т.д.

2.3 Уставной/Правовой/Не соблюдение договоров

Ущерб нанесен невозможностью выполнения правовых, нормативных и договорных обязательств, нарушением договора с третьими сторонами, стоимостью судебных разбирательств и штрафами.

3. Ущерб физическим лицам

Ущерб, нанесенный третьим лицам, использующим систему, в силу наличия в ней слабых мест и рисками информации, находящейся в системе.

3.1 Финансовые потери

Ущерб, повлекший прямые финансовые потери для третьих лиц или персонала, работающих в системе или использующих ее для ведения дел.

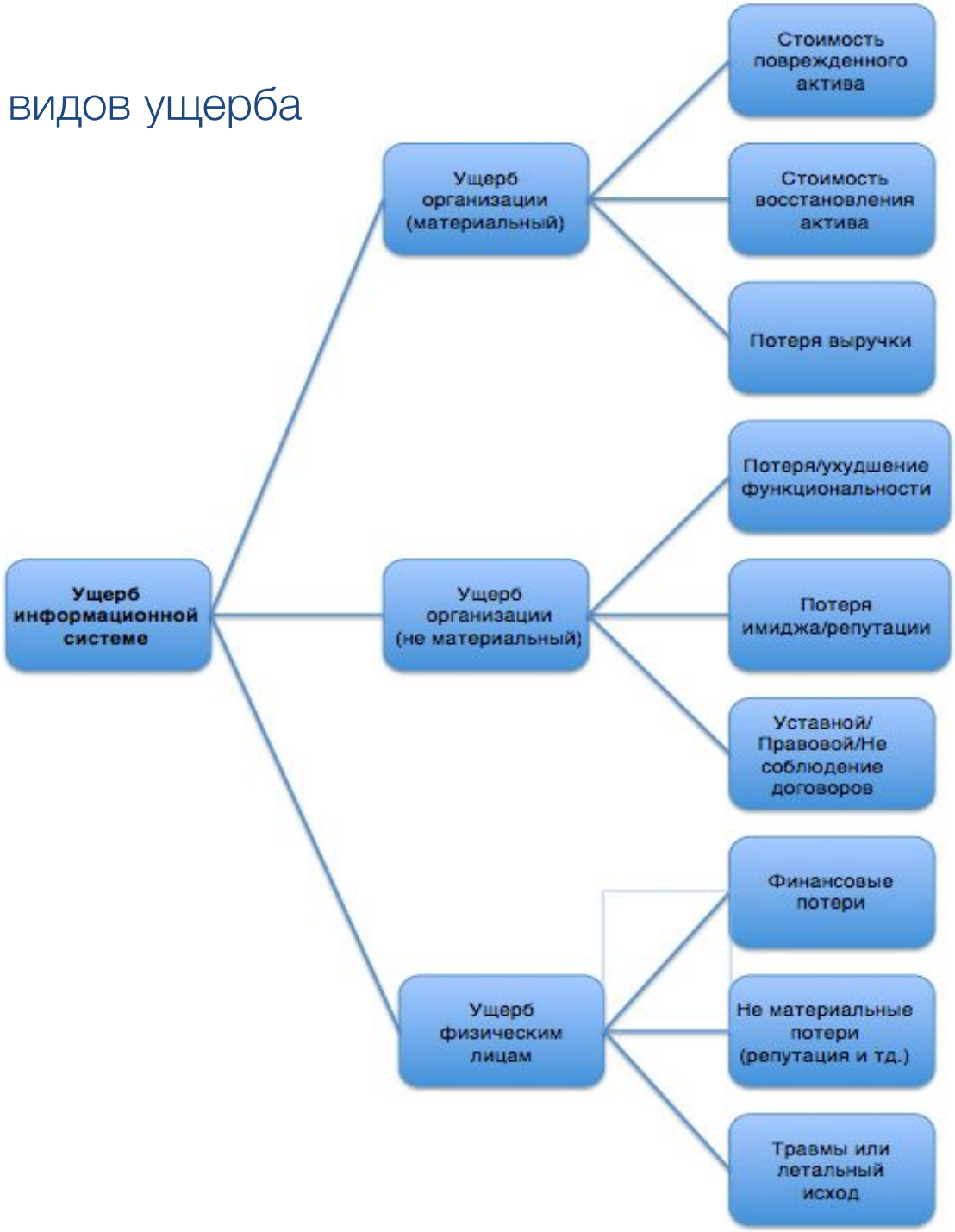
3.2 Не материальные потери

Ущерб, повлекший нематериальный ущерб, такой как нарушение неприкосновенности частной жизни, преследования и тд. третьих лиц использующих систему, или персонала, работающего в ней.

3.3 Травмы или летальный исход

Ущерб, повлекший за собой травмы или смерть третьих лиц в силу наличия слабых мест в системе или подвергания риску информации, находящейся в ней.

Взаимосвязь видов ущерба



Шаг 1: Оценка «Материального ущерба организации» в зависимости от показателей ‘стоимость поврежденного актива’, ‘стоимость восстановления’ и ‘потеря выручки.

Определите уровень показателя ‘*стоимость поврежденного актива*’, в зависимости от уровня ожидаемого ущерба, нанесенного из-за нарушения безопасности.

минимальный ущерб – 1,

значительный ущерб – 2,

катастрофический ущерб – 3.

отсутствия ущерба – значение 0.

Определите значение показателя ‘*стоимость восстановления*’, в зависимости от ожидаемой стоимости восстановления, которого требует нарушенная безопасность.

минимальная стоимость – 1,

умеренная стоимость – 2,

высокая стоимость – 3.

если средства для восстановления не привлекаются– значение 0.

Определите значения показателя ‘*потеря выручки*’, в зависимости от уровня ожидаемой потери выручки, вызванной нарушением безопасности.

минимальные потери – 1,

значительные потери – 2,

катастрофические потери – 3.

В случае отсутствия потерь выручки – значение 0.

Просуммируйте три полученных значения для нахождения Материального Ущерба Организации в таблице 1.

Шаг 2: Оценка не материального ущерба организации» в зависимости от показателей ‘потеря/ухудшение функциональности’, ‘потеря имиджа/репутации’ и ‘последствия уставного/правового/несоблюдения договоров’.

Определить значения показателя ‘*потеря/ухудшение функциональности*’, в зависимости от уровня ожидаемой потери/ухудшения, вызванного нарушением безопасности.

не значительное ухудшение – 1,

значительное ухудшение – 2,

полная потеря – 3.

В случае сохранения функциональности на прежнем уровне – значение 0.

Определите значения показателя ‘потеря имиджа/репутации’, в зависимости от ожидаемого уровня потери имиджа/репутации, вызванной нарушением безопасности.

минимальный уровень потерь – 1.

значительный уровень потерь – 2.

Серьезный уровень или полная потеря имиджа/репутации – 3.

В случае сохранения прежнего уровня имиджа/репутации – значение 0.

Просуммируйте три полученных значения для нахождения Не материального Ущерба Огранизации в таблице 1.

Шаг 3: Оценка «Ущерба физическим лицам» в зависимости от показателей ‘финансовые потери’, ‘не материальные потери’ и ‘травмы и летальный исход’.

Определите значения показателя ‘финансовые потери’, в зависимости от уровня ожидаемых потерь, вызванных нарушением безопастности.

минимальные потери – 1.

существенные потери – 2.

Очень существенные потери – 3.

отсутствие финансовых потерь –0.

Определите значение показателя ‘не материальные потери’, в зависимости от уровня ожидаемых потерь, вызванных нарушением системы безопасности.

минимальные потери – 1.

существенные потери – 2.

критические потери – 3.

отсутствие не материальных потерь –0.

Определите значения показателя ‘травмы и летальный исход’, в зависимости от ожидаемого уровня вероятности травмирования и летальных исходов, вызванных нарушением безопасности.

небольшие травм – 1.

серьезное травмирование – 2.

смерть физических лиц – 3.

избежания травм и летальных исходов – 0.

Просуммируйте три полученных значения для нахождения Ущерба физическим лицам Организации в таблице 1.

Таблица 1: Матрица ущерба 1

Общее значение	Уровень ущерба
0-4	НИЗКИЙ
5-6	СРЕДНИЙ
7-9	ВЫСОКИЙ

Шаг 4: Определить значение общего ущерба для Информационной системы, в зависимости от показателей
‘Материальный ущерб организации’,
‘Не материальный ущерб организации’ и
‘Ущерб физическим лицам’, учитывая наивысшие показатели ущерба (Таблица 2),
Результат и является уровнем критичности Информационной системы.

Таблица 2: Матрица ущерба 2

Уровень Материального ущерба Организации	Уровень Не материального ущерба Организации	Уровень Ущерба физическим лицам	Уровень Совокупного ущерба Информационной системе
НИЗКИЙ	НИЗКИЙ	НИЗКИЙ	НИЗКИЙ
НИЗКИЙ	НИЗКИЙ	СРЕДНИЙ	СРЕДНИЙ
НИЗКИЙ	НИЗКИЙ	ВЫСОКИЙ	ВЫСОКИЙ
НИЗКИЙ	СРЕДНИЙ	НИЗКИЙ	СРЕДНИЙ
НИЗКИЙ	СРЕДНИЙ	СРЕДНИЙ	СРЕДНИЙ
НИЗКИЙ	СРЕДНИЙ	ВЫСОКИЙ	ВЫСОКИЙ
НИЗКИЙ	ВЫСОКИЙ	НИЗКИЙ	ВЫСОКИЙ
НИЗКИЙ	ВЫСОКИЙ	СРЕДНИЙ	ВЫСОКИЙ
НИЗКИЙ	ВЫСОКИЙ	ВЫСОКИЙ	ВЫСОКИЙ
СРЕДНИЙ	НИЗКИЙ	НИЗКИЙ	СРЕДНИЙ
СРЕДНИЙ	НИЗКИЙ	СРЕДНИЙ	СРЕДНИЙ
СРЕДНИЙ	НИЗКИЙ	ВЫСОКИЙ	ВЫСОКИЙ
СРЕДНИЙ	СРЕДНИЙ	НИЗКИЙ	СРЕДНИЙ
СРЕДНИЙ	СРЕДНИЙ	СРЕДНИЙ	СРЕДНИЙ
СРЕДНИЙ	СРЕДНИЙ	ВЫСОКИЙ	ВЫСОКИЙ
СРЕДНИЙ	ВЫСОКИЙ	НИЗКИЙ	ВЫСОКИЙ
СРЕДНИЙ	ВЫСОКИЙ	СРЕДНИЙ	ВЫСОКИЙ
СРЕДНИЙ	ВЫСОКИЙ	ВЫСОКИЙ	ВЫСОКИЙ
ВЫСОКИЙ	НИЗКИЙ	НИЗКИЙ	ВЫСОКИЙ
ВЫСОКИЙ	НИЗКИЙ	СРЕДНИЙ	ВЫСОКИЙ
ВЫСОКИЙ	НИЗКИЙ	ВЫСОКИЙ	ВЫСОКИЙ
ВЫСОКИЙ	СРЕДНИЙ	НИЗКИЙ	ВЫСОКИЙ
ВЫСОКИЙ	СРЕДНИЙ	СРЕДНИЙ	ВЫСОКИЙ
ВЫСОКИЙ	СРЕДНИЙ	ВЫСОКИЙ	ВЫСОКИЙ
ВЫСОКИЙ	ВЫСОКИЙ	НИЗКИЙ	ВЫСОКИЙ
ВЫСОКИЙ	ВЫСОКИЙ	СРЕДНИЙ	ВЫСОКИЙ
ВЫСОКИЙ	ВЫСОКИЙ	ВЫСОКИЙ	ВЫСОКИЙ

Таблица 3: Пример оценки уровня критичности информационной системы «AGMARKNET»

Название приложения Электронного правительства	AGMARKNET	
Связанное с ним министерство	Министерство сельского хозяйства	
Цель	Целью AGMARKNET является контакт оптовых рынков сельскохозяйственной продукции для обмена рыночной информацией. Портал AGMARKNET был развит для укрепления интерфейсов (связей) между поставщиками сельскохозяйственных товаров относящихся к государственным и не государственным организациям, фермерами, торговцами, экспортерами, политиками, академическими институтами и т.д. (http://www.agmarknet.nic.in)	
Шаг 1: Оценка материального ущерба организации	а. Стоимость поврежденного актива	1
	б. Стоимость восстановления	1
	в. Потеря выручки	0
	Сумма (а+б+в)	2
	Уровень материального ущерба организации	НИЗКИЙ
Шаг 2: Оценка не материального ущерба организации	а. Потеря/ухудшение функциональности	2
	б. Потеря имиджа/репутации	2
	в. Уставной/Правовой/Не соблюдение договоров	2
	Сумма (а+б+в)	6
	Уровень не материального ущерба организации	СРЕДНИЙ
Шаг 3: Оценка ущерба физическим лицам	а. Финансовые потери	1
	б. Не материальные потери	2
	в. Травмы и летальный исход	0
	Сумма (а+б+в)	3
	Уровень ущерба физическим лицам	НИЗКИЙ
Шаг 4: Оценка ущерба Информационной системе/Категоризация безопастности	Уровень материального ущерба организации	**НИЗКИЙ**
	Уровень не материального ущерба организации	**СРЕДНИЙ**
	Уровень ущерба физическим лицам	**НИЗКИЙ**
	КАТЕГОРИЯ БЕЗОПАСНОСТИ: СРЕДНИЙ УРОВЕНЬ УЩЕРБА	

Таблица 4: Пример оценки уровня критичности информационной системы «ePost»

Название приложения Электронного правительства	ePost	
Связанное с ним министерство	Министерство сообщения	
Цель	Сообения могут быть посланы куда бы то ни было в Индии с помощью почтовых отделений используя программной обеспечение ePost (http://indiapost.nic.in)	
Шаг 1: Оценка материального ущерба организации	а. Стоимость поврежденного актива	1
	б. Стоимость восстановления	1
	в. Потеря выручки	3
	Сумма (а+б+в)	5
	Уровень материального ущерба организации	СРЕДНИЙ
Шаг 2: Оценка не материального ущерба организации	а. Потеря/ухудшение функциональности	2
	б. Потеря имиджа/репутации	3
	в. Уставной/Правовой/Не соблюдение договоров	2
	Сумма (а+б+в)	7
	Уровень не материального ущерба организации	ВЫСОКИЙ
Шаг 3: Оценка ущерба физическим лицам	а. Финансовые потери	1
	б. Не материальные потери	2
	в. Травмы и летальный исход	0
	Сумма (а+б+в)	3
	Уровень ущерба физическим лицам	НИЗКИЙ
Шаг 4: Оценка ущерба Информационной системе/Категоризация безопастности информационной системы	Уровень материального ущерба организации	**СРЕДНИЙ**
	Уровень не материального ущерба организации	**ВЫСОКИЙ**
	Уровень ущерба физическим лицам	**НИЗКИЙ**
	КАТЕГОРИЯ БЕЗОПАСНОСТИ: ВЫСОКИЙ УРОВЕНЬ УЩЕРБА	

Заполните таблицу самостоятельно:

Название приложения Электронного правительства		
Связанное с ним министерство		
Цель		
Шаг 1: Оценка материального ущерба организации	а. Стоимость поврежденного актива	
	б. Стоимость восстановления	
	в. Потеря выручки	
	Сумма (а+б+в)	
	Уровень материального ущерба организации	
Шаг 2: Оценка не материального ущерба организации	а. Потеря/ухудшение функциональности	
	б. Потеря имиджа/репутации	
	в. Уставной/Правовой/Не соблюдение договоров	
	Сумма (а+б+в)	
	Уровень не материального ущерба организации	
Шаг 3: Оценка ущерба физическим лицам	а. Финансовые потери	
	б. Не материальные потери	
	в. Травмы и летальный исход	
	Сумма (а+б+в)	
	Уровень ущерба физическим лицам	
Шаг 4: Оценка ущерба Информационной системе/Категоризация безопастности информационной системы	Уровень материального ущерба организации	
	Уровень не материального ущерба организации	
	Уровень ущерба физическим лицам	
	КАТЕГОРИЯ БЕЗОПАСНОСТИ:	

Благодарю за внимание!