Управление операционной надежностью и кибер-риски

Окулесский Василий Андреевич, к.т.н.,
Советник Службы информационной безопасности
АО «БМ-Банк»

Выбор пути в ИБ

Для системы ИБ всегда ключевым моментом был выбор целей и определение задач.

На сегодня ключевой вектор :

Цели безопасности – неотъемлемая составная часть целей бизнеса.

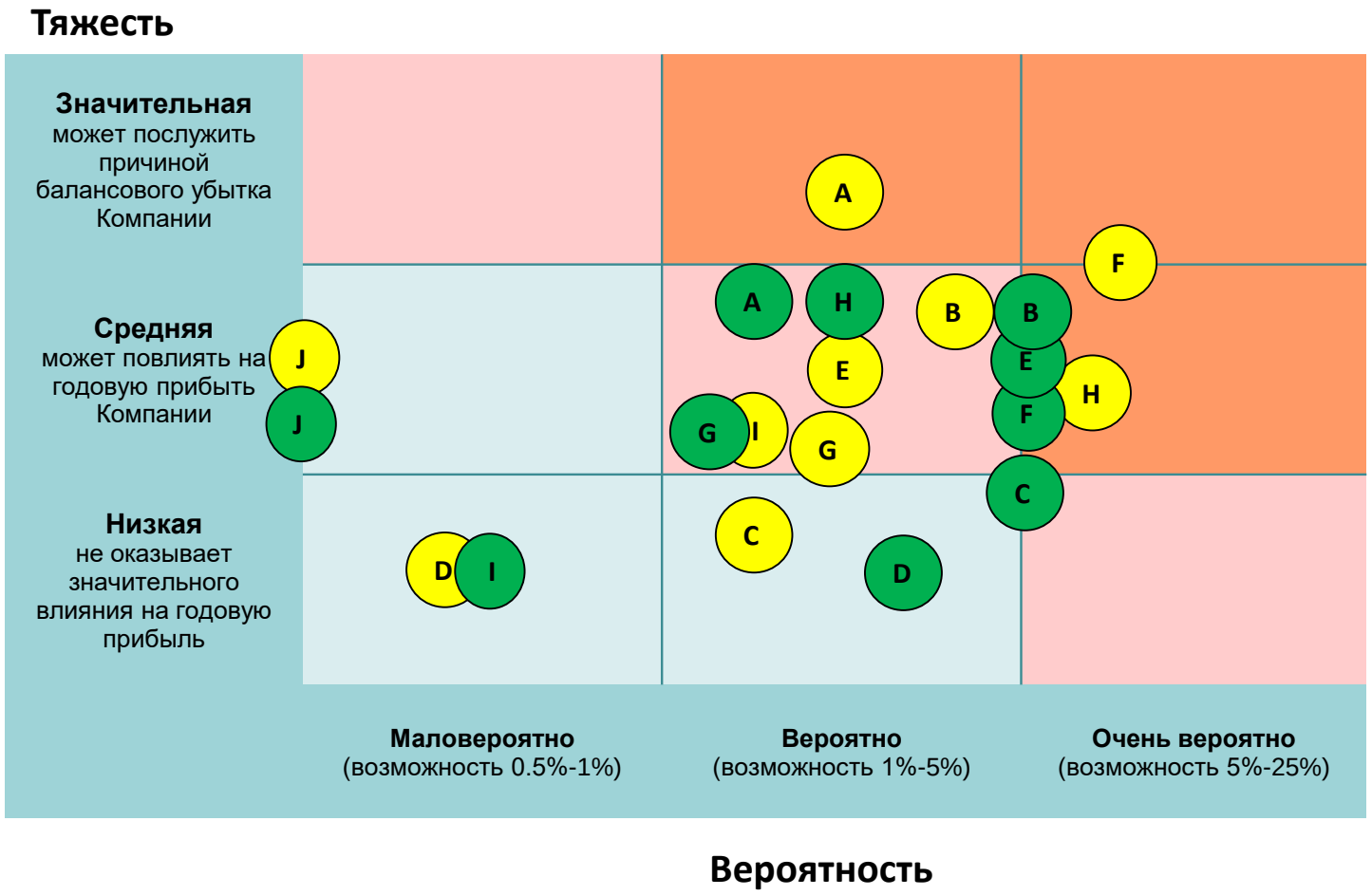
Более того, интеграция ИБ с другими видами безопасности привела к необходимости комплексного формирования целей ИБ, а специфика методов и технологий ИБ должна учитываться в рамках конкретных задач.

Профиль рисков для различных типов банков

- небольшие банки

- крупные банки

A	Кража интеллектуальной собственности
B	Перерыв в деятельности
C	Утрата данных и программного обеспечения
D	Кибер-вымогательство
E	Кража денег
F	Нарушение конфиденциальности
G	Ответственность перед третьими лицами
H	Ущерб репутации
I	Гибель и повреждение имущества
J	Вред жизни и здоровью



***По материалам брокера Guy Carpenter, London**

** **Перерыв в деятельности, кража денег, нарушение конфиденциальности (в т.ч. персональных данных) и утрата ПО** – наиболее вероятные риски для предприятий среднего и малого бизнеса

Главная идея поляны

Требования последних редакций 716-П и 719-П делают, по сути, *революцию в оценке значимости ИБ для банка*. Влияние результата оценки на расчет дополнительного резервного капитала банка переносит ответственность за организацию ИБ со специализированного подразделения непосредственно на руководство банка.

При этом оценка риска ИБ должна стать главным показателем бизнес-оценки состояния системы ИБ

787-П дает один из значимых инструментов формирования измеряемых параметров

Почему идея может не работать

Если это не решить, дальше можно не читать

Существующая модель оценки операционного риска методологически не может быть применена впрямую для оценки риска киберугроз

Применимая сейчас в большинстве банков **качественная модель оценки риска** не дает бизнес-оценки, а для формирования финансовой модели – отсутствуют единые методики.

Нужна прозрачная методика оценки потенциального *финансового* ущерба от возможной реализации киберугроз

Подводные камни

Какие ИС могут попасть в скоуп мониторинга

Все системы класса МС/ВС

Все системы, связанные с обеспечением функционирования инфраструктуры (в т.ч. ИТ-системы мониторинга инфраструктуры)Все системы, что связаны с управлением доступом к Информационным Активам

Системы мониторинга и анализа событий (инцидентов) ИБ

Системы контроля утечек конфиденциальной информации, включая инциденты в системах документооборота

Операционная надежность источник контролируемых параметров

Как получить контролируемые параметры

ID	Краткое название показателя	Наименование технологического процесса	Сигнальное значение 2022	Контрольное значение 2022	Единица измерения
ЦПОН_1	Доля деградации технологического процесса	Технологический процесс, обеспечивающий привлечение денежных средств юридических лиц во вклады	75	95	%
		Технологический процесс, обеспечивающий размещение привлеченных во вклады денежных средств физических и (или) юридических лиц от своего имени и за свой счет	75	95	%
		Технологический процесс, обеспечивающий осуществление переводов денежных средств по поручению физических лиц по их банковским счетам	75	95	%
		Технологический процесс, обеспечивающий осуществление переводов денежных средств по поручению юридических лиц, в том числе банков-корреспондентов, по их банковским счетам, за исключением переводов по распоряжениям участников платежной системы	75	95	%
		Технологический процесс, обеспечивающий открытие и ведение банковских счетов физических лиц	75	95	%
		Технологический процесс, обеспечивающий открытие и ведение банковских счетов юридических лиц	75	95	%
		Технологический процесс, обеспечивающий выполнение операций на финансовых рынках	75	95	%
		Технологический процесс, обеспечивающий выполнение кассовых операций	75	95	%
		Технологический процесс, обеспечивающий работу онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций	75	95	%
		Технологический процесс, обеспечивающий размещение и обновление биометрических персональных данных в единой биометрической системе	75	95	%

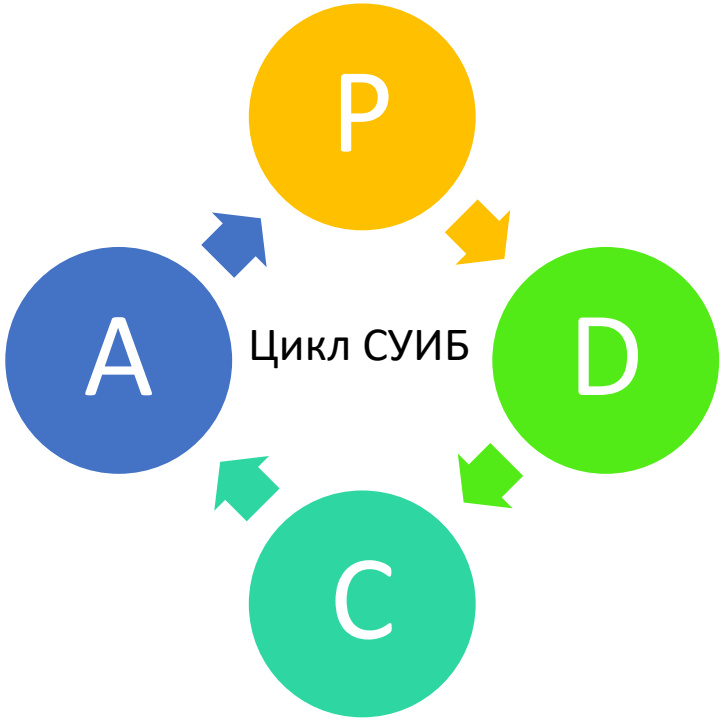
Как получить контролируемые параметры

Система		Fraud Detection						
IP-адрес		192.168.46.ZZZ (Сервер приложения основной)	192.168.46.XXX (Сервер БД основной)					
DNS-имя		SL0XXX	SL0УУУ					
Назначение		Антифрод система						
Тип		Сервер	Сервер					
Операционная система		RHEL 7	RHEL 7.9					
Ответственное за систему подразделение		СИБ						
Ответственное за инфраструктуру подразделение		ДИТ						
Дни оповещений		круглосуточно						
Время оповещений		00-00:24-00						
№ п/п	Сервер	Метрика	Способ контроля	Частота контроля	Нормальное состояние (Cleared Alarm)	Пороговое Значение (Minor Alarm)	Пороговое Значение (Major Alarm)	Пороговое Значение (Critical Alarm)
1	Server Thresholds							
	CPU Utilization	Процессор	SNMP	1 мин	нет	нет	нет	нет
	Memory Utilization	RAM	SNMP	1 мин	нет	нет	нет	нет
№ п/п	Ресурсы/Процессы/Тесты	Метрика	Способ контроля	Частота контроля	Нормальное состояние (Cleared Alarm)	Пороговое Значение (Minor Alarm)	Пороговое Значение (Major Alarm)	Пороговое Значение (Critical Alarm)
2	File Systems (Ресурсы Сервера)							
	Дисковое пространство C:\ (Система)	HDD	SNMP	? мин	91%	92%	96%	99%
	Virtual Memory		SNMP	? мин	нет	нет	нет	нет
3	Processes (Процессы Сервера)							
	????.exe	Windows Service	SNMP	? мин	?	?	?	?
4	Service Performance Manager (Тесты)							
	IP Address 192.168.46.24	Доступность	ICMP	? мин	0.0% Loss	? % Loss	? % Loss	SPM Timeout Event
	IP Address:Port 192.168.46.24:18080	Доступность	TCP	? мин	0.0% Loss	? % Loss	? % Loss	SPM Timeout Event
	Address http:// 192.168.46.24:18080	Доступность	HTTP	? мин	0.0% Loss	? % Loss	? % Loss	SPM Timeout Event
	Address https:// -----	Доступность	HTTPS	? мин	0.0% Loss	? % Loss	? % Loss	SPM Timeout Event
	SQL DataBase Server:	Доступность	SQL Query	? мин	0.0% Loss	? % Loss	? % Loss	SPM Timeout Event
	Database Name:							
	User Name:							
	Password:							
	Query String:							
	Destination Port:							

Как это может работать

Оценка рисков = разработка плана ИБ
и **набора контролируемых показателей**

Разработка плана совершенствования системы ИБ для снижения (поддержания) принятого уровня риска



Мониторинг выбранных показателей системами on-line мониторинга

Периодическая (плановая и неплановая) оценка риска и состояния ИБ при проведении оценок соответствия требованиям регуляторов (в том числе при проведении надзорных мероприятий)