Российские Наукоёмкие Технологии

«О требованиях регулятора в части управления рисками информационной безопасности в кредитной организации»

Взгляд эксперта

Курило А.П.
Заместитель генерального директора
АО «РНТ», КТН

2018 г.

Ключевые свойства информации и что из этого следует

1

Инвариантность к вопросам безопасности

- Мир, в котором существует информация как сущность содержит понятия точность, актуальность, достоверность, объективность и т.д. и не включает понятия секретность и защищенность

Изменчивость

Существование только в объектной среде, ранее, только на материальном носителе (бумага, глина, камень, металл

Ценность

Неуничтожаемость

2

Свойства безопасности придаются информации через свойства объектной среды, в результате чего:

- Оценки защищенности информации носят косвенный характер, так как оценивается не защищенность информации, а специфические свойства объектной среды
- Все оценки носят вероятностный характер

3

Ключевые свойства объектной среды:

- Сложность
- Изменчивость
- Наличие уязвимостей
- Не прозрачность
- Плохая сохраняемость информации

Объект среды информационного актива: Материальный объект среды использования и (или) эксплуатации информационного актива (объект хранения, передачи, обработки, уничтожения и т.д.). (СТО ИББС 1.0)

Ключевая задача:

эффективный контроль свойств объектной среды, обеспечивающей безопасность информации с учетом особенностей этой среды.

Эволюция подходов к созданию нормативной базы по информационной безопасности

Красная книга

Положение по защите от НСД

Открытые критерии

BS 1779

Документы ЕС по ЭП и ПД

Общие критерии

ГОСТы Р 2700х

НМД ФСБ и ФСТЭК

ISO 2700x

УК РФ, ГК РФ, ФЗ 161-ФЗ
ФЗ 162-ФЗ, ФЗ 152-ФЗ
ФЗ 63-ФЗ, ФЗ 187-ФЗ, ФЗ 86-ФЗ,

Проект Положения о требованиях к КФО

СТО ИББС

Базель 2

PSI DCC

382-П

Проект Положения об управлении операционными рисками

ГОСТ Р 57580.1-2017

Базель 3

Базовый методический подход, реализованный в НМД первого поколения. Цели и результаты

Цели

1. Через выставление конкретных требований по безопасности парировать ключевые недостатки объектной среды, такие как: **сложность, наличие уязвимостей, не прозрачность, плохая сохраняемость информации.**
2. Через организацию действенного контроля парировать такой ключевой недостаток объектной среды, как **изменчивость среды**, приводящую к утрате свойств безопасности.

В основу принципов контроля были положены механизмы регулярной оценки уровня информационной безопасности кредитной организации внешней стороной (аудит) и самооценки.

Результаты

Практика выявила следующее:

a. Разработанный методический аппарат имел достаточную точность, однако погрешность измерений сильно зависела от качества работы аудитора, проводящего оценку. Оказался слишком велик субъективный фактор.

b. Самооценка столкнулась с массовыми искажениями результатов.

c. КО потеряли интерес к проведению работ, так как выполнение аудита и самооценки не давало никаких бизнес-преференций.

d. Итоговая оценка фактически не учитывала вероятностную сущность процесса противодействия угрозам в информационной сфере.

e. Проведение Банком России работ по установлению требований по информационной безопасности и контролю требует законодательной поддержки.

Усовершенствованный базовый методический подход, заложенный в НМД второго поколения

1. **Набор требований по обеспечению безопасности, представленных в ГОСТ Р 57580.1-2017 в настоящее время отработан, представляется полным и соответствующим мировой практике.**
2. Готовится второй стандарт.
3. Подготовлен проект Положения Банка России «ОБ УСТАНОВЛЕНИИ ОБЯЗАТЕЛЬНЫХ ДЛЯ НЕКРЕДИТНЫХ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ДЕЯТНЛЬНОСТИ ВСФЕРЕ ФИНАНСОВЫХ РЫНКОВ».
4. Подготовлен проект Положения Банка России «О ТРЕБОВАНИЯХ К СИСТЕМЕ УПРАВЛЕНИЯ ОПЕРАЦИОННЫМ РИСКОМ В КРЕДИТНОЙ ОРГАНИЗАЦИИ И БАНКОВСКОЙ ГРУППЕ»

Цели совершенствования НМД:

Создание по-настоящему эффективной системы обеспечения информационной безопасности в КО, банковской группе и НФО за счет:

1. Учета вероятностной сущности процессов обеспечения информационной безопасности и результатов оценки через механизмы управления рисками информационной безопасности, отнесенными к группе операционных рисков.
2. Совершенствования методологии и организационно-правовых процедур контроля с целью повышения корректности результатов.
3. Создания заинтересованности у КО, банковской группы, в проведении работ по обеспечению ИБ путем введения механизма уменьшения размера капитала, необходимого для покрытия потерь от операционного риска (далее – необходимый капитал) в рамках внутренних процедур оценки достаточности капитала (далее – ВПОДК).

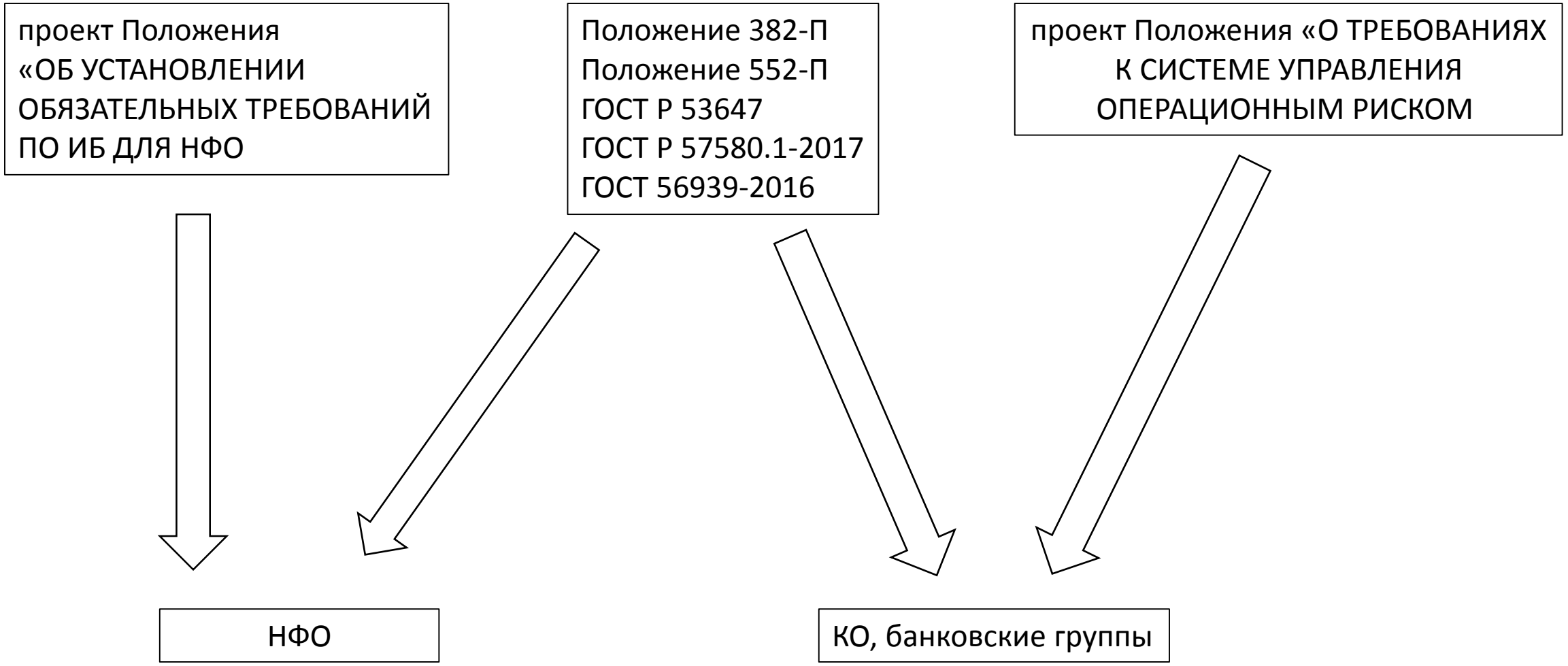
Правовая основа: ФЗ№ 86-ФЗ

Статья 57.4. Банк России по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, **устанавливает обязательные для кредитных организаций требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента,** за исключением требований к обеспечению защиты информации, установленных федеральными законами и принятыми в соответствии с ними нормативными правовыми актами.

Структура деятельности в соответствии с появляющейся НМД

1. Реализация требований по безопасности и контролю

2. Реализация требований по управлению рисками



Реализация требований по безопасности и контролю

1. Требования, обеспечивающие выполнение защитных мер являются стандартными и соответствуют мировой практике.
2. Новое требование по сертификации блоков АБС по требованиям ФСТЭК
3. Периодичность контроля и проверок:
   - a. Однократно (с некоторыми оговорками) - Сертификация АБС

     1 раз в 2 года - проведение оценки соответствия требованиям безопасности.
   - b. Ежегодно :
     - Пентестирование
     - Сканирование уязвимостей.
4. Оценка соответствия выполняется по четырехбальной шкале.
5. Оценка проводится:
   - Внешней стороной
   - В виде самооценки
   - Силами ЦБ
6. Внешняя организация, привлекаемая для проверок и тестирования, должна иметь Лицензию ФСТЭК на работу по защите конфиденциальной информации.

Реализация требований по управлению рисками

1. Кредитная организация (головная кредитная организация банковской группы), создает систему и определяет порядок управления риском информационной безопасности.
2. Кредитная организация (головная кредитная организация банковской группы) определяет систему управления риском Информационных систем.
3. Разрабатываются Политики управления рисками ИБ и ИС, и ряд документов, устанавливаются регулярные процедуры их пересмотра.
4. Ведется внутренняя отчетность, включая результаты проверок выполнения требований безопасности.
5. Используется лицензионное и сертифицированное ПО.
6. Проводятся регулярные (не реже 1 раза в год) оценки состава компонент, архитектуры, инфраструктуры и характеристик ИС на их достаточность и эффективность для обеспечения функционирования ключевых бизнес-процессов.
7. Вводится мониторинг операционного риска.
8. Вводится процедура самооценки операционного риска на регулярной основе.
9. Проводится экспертная профессиональная оценка уровня операционного риска.
10. Кредитная организация (головная кредитная организация банковской группы) разрабатывает во внутренних документах методику сценарного анализа операционных рисков и порядок его проведения.
11. Надзорная оценка системы управления рисками со стороны ЦБ – ежегодно/
12. Создается аналитическая база данных о событиях операционного риска и потерях, включая события ИС и ИБ.
13. Создается классификатор событий и потерь (прямые, косвенные и качественные).

Стимул на основе схемы расчета капитала на покрытие рисков ИБ и ИС

В соответствии с указаниями Указания Банка России № 3624-У выбирается:

- регуляторный подход на базе расчета минимального регуляторного капитала на покрытие операционного риска на основе Положения Банка России № 346-П и прогнозных сценариев среднегодовых потерь от реализации событий операционного риска и событий риска ИБ;
- подход на базе внутренних моделей количественной оценки потерь от реализации операционного риска на основе статистики базы данных о событиях операционного риска и событий риска ИБ (с использованием статистики за период не менее 5 лет) с использованием методов, применяемых в международной практике.

В первом случае - дельта капитала на покрытие рисков ИБ и ИС определяется на основании сценарного моделирования.

Во втором случае дельта может быть принята равной нулю на основании мотивированного суждения службы управления рисками об отсутствии факторов возможных потерь.

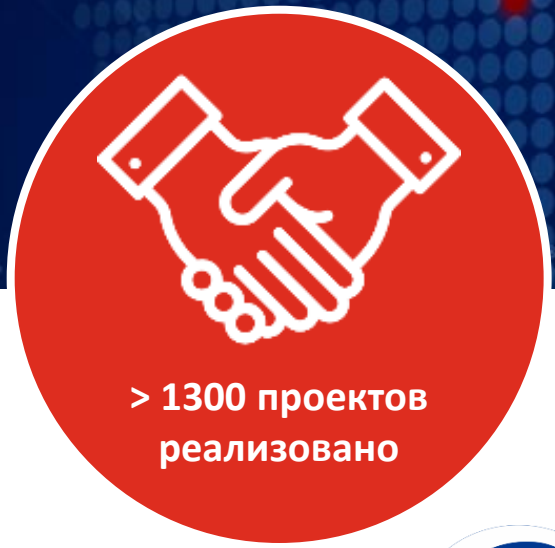
В обоих случаях используются результаты проверок и оценок соответствия.

Оба этих фактора являются стимулирующими для руководства КО.

Все остальное это уже конкретные схемы действий.

АО «РНТ» – надежный поставщик продуктов и услуг в области ИБ для государственных и коммерческих организаций

Среди постоянных заказчиков - органы государственной власти и управления, силовые структуры Российской Федерации, крупнейшие государственные и коммерческие компании



Благодарю за внимание

Курило Андрей,
kap@rnt.ru

+7 (495) 777-75-77
sales@rnt.ru
www.rnt.ru