РЕКОМЕНДАЦИИ В ОБЛАСТИ
СТАНДАРТИЗАЦИИ
БАНКА РОССИИ

РС БР ИББС-2.7-2015

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дата введения: 2015-05-01

Москва
2015

Предисловие

ВВЕДЕНЫ в действие приказом Банка России от 19 февраля 2015 года № ОД-392.

Содержание

Введение

Одним из основных условий удовлетворения текущих и перспективных потребностей организации банковской системы (БС) Российской Федерации (РФ) в обеспечении информационной безопасности (ИБ) является наличие достаточных для этого ресурсов и их эффективное использование.

В действующем стандарте Банка России СТО БР ИББС-1.0 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” (далее – СТО БР ИББС-1.0) установлены требования о принятии руководством организации БС РФ решений о выделении ресурсов, необходимых для планирования, реализации, выполнения, проверки и совершенствования (далее при совместном упоминании – обеспечение) процессов системы обеспечения ИБ организации БС РФ (далее – СОИБ).

Настоящий документ устанавливает рекомендации по определению потребностей организации БС РФ в ресурсах, необходимых для обеспечения процессов СОИБ (далее – ресурсы ИБ), и по проведению контроля эффективности использования этих ресурсов.

Устанавливаемые рекомендации направлены на поддержание применения СТО БР ИББС-1.0 в части реализации системы менеджмента ИБ организации БС РФ (далее – СМИБ) и поддержание процесса реализации требований к обеспечению ИБ, установленных в СТО БР ИББС-1.0 и нормативных актах Банка России.

РЕКОМЕНДАЦИИ В ОБЛАСТИ СТАНДАРТИЗАЦИИ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дата введения 2015-05-01

1. Область применения

Настоящий документ распространяется на организации БС РФ и устанавливает рекомендации по определению потребностей организации БС РФ в ресурсах ИБ и контролю эффективности их использования.

Настоящий документ рекомендован для применения путем использования установленных в нем положений, а также путем включения ссылок на них и (или) их прямого использования во внутренних документах организации БС РФ.

Рекомендации по определению потребностей организации БС РФ в ресурсах ИБ и контролю эффективности их использования, установленные в настоящем документе, могут, если иное не указанно явно, применяться при реализации требований к обеспечению ИБ, установленных законодательством РФ, в том числе нормативными актами Банка России, СТО БР ИББС-1.0.

Настоящий документ применяется организациями БС РФ на добровольной основе. В конкретной организации БС РФ для определения потребностей в ресурсах ИБ могут использоваться иные подходы, отражающие специфику и сложившуюся практику организации БС РФ в ресурсном обеспечении ИБ.

2. Нормативные ссылки

В настоящих рекомендациях в области стандартизации Банка России использованы нормативные ссылки на следующие документы:

СТО БР ИББС-1.0;

РС БР ИББС-2.2 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности” (далее – РС БР ИББС-2.2).

3. Термины и определения

В настоящих рекомендациях применяются термины в соответствии со СТО БР ИББС-1.0, а также следующие термины с соответствующими определениями:

3.1. **Ресурс ИБ** – кадровые ресурсы (персонал) службы ИБ и финансовые средства, необходимые для планирования, реализации, выполнения, проверки и совершенствования процессов СОИБ с целью обеспечения целевого уровня обеспечения ИБ.

3.2. **Ресурсное обеспечение ИБ** – процесс управления, обеспечивающий определение потребностей в ресурсах ИБ и контроль эффективности использования ресурсов ИБ.

3.3. **Уровень зрелости выполнения процесса СОИБ** – мера оценки полноты, адекватности и эффективности выполнения процесса СОИБ.

4. Обозначения и сокращения

АБС – автоматизированная банковская система;
БС – банковская система;
ИБ – информационная безопасность;
РФ – Российская Федерация;
СОИБ – система обеспечения информационной безопасности;
СМИБ – система менеджмента информационной безопасности.

5. Общие положения

5.1. Основными целями реализации ресурсного обеспечения ИБ, рассматриваемыми в настоящем документе, являются:

– обеспечение процессов СОИБ финансовыми средствами;
– обеспечение службы ИБ организации БС РФ кадровыми ресурсами, необходимыми и достаточными для реализации процессов СОИБ;
– контроль эффективности использования ресурсов ИБ.

5.2. Потребности в обеспечении процессов СОИБ ресурсами ИБ рекомендуется определять на основе предполагаемой величины возможного ущерба (финансового эквивалента возможных потерь) организации БС РФ в случае реализации актуальных для организации БС РФ рисков нарушения ИБ.

Организации БС РФ рекомендуется обеспечить надлежащий баланс между актуальными рисками нарушения ИБ, связанными с наличием уязвимостей в выполнении процессов СОИБ, и ресурсами ИБ, используемыми для обеспечения целевого уровня ИБ и, соответственно, направленными на снижение указанных рисков.

5.3. Для определения потребностей в обеспечении процессов СОИБ ресурсами ИБ в организации БС РФ рекомендуется использование методик оценки актуальных рисков нарушения ИБ в количественной (денежной) форме. Указанные методики рекомендуется разрабатывать для учета влияния рисков нарушения ИБ на основную деятельность организации БС РФ через предполагаемую величину возможного ущерба (финансового эквивалента возможных потерь) организации БС РФ в случае реализации актуальных для организации БС РФ рисков нарушения ИБ.

Для оценки рисков нарушения ИБ в количественной (денежной) форме рекомендуется использовать РС БР ИББС-2.2.

5.4. Снижение рисков нарушения ИБ обеспечивается минимизацией уязвимостей в выполнении процессов СОИБ, направленных на непосредственное обеспечение ИБ, путем повышения их уровня зрелости. Повышение уровня зрелости выполнения процессов СОИБ достигается планированием, реализацией, выполнением, поверкой и совершенствованием процессов СОИБ – выполнением для каждого управляемого процесса СОИБ деятельности в рамках СМИБ.

Неполнота выполнения процессов СМИБ создает уязвимости при выполнении управляемых процессов СОИБ, что, в свою очередь, увеличивает риски для основной деятельности организации БС РФ.

Ресурсы ИБ являются одним из основных факторов, определяющих полноту и качество выполнения процессов СМИБ, которые, в свою очередь, определяют уровень зрелости выполнения управляемых процессов СОИБ.

5.5. Для реализации ресурсного обеспечения ИБ организации БС РФ рекомендуется:

– установить и применять методологию оценивания уровня зрелости выполнения процессов СОИБ. Рекомендации к методологии оценивания уровня зрелости выполнения процессов СОИБ установлены в разделе 6 настоящего документа;
– установить и применять методологию оценивания рисков нарушения ИБ с учетом данных о реализованном организацией БС РФ уровне зрелости выполнения процессов СОИБ. Рекомендации к методологии оценивания рисков нарушения ИБ установлены в разделе 7 настоящего документа;
– обеспечить целевой уровень обеспечения ИБ путем повышения уровня зрелости выполнения процессов СОИБ до значения, реализующего снижение рисков нарушения ИБ до допустимого уровня. Повышение уровня зрелости выполнения процессов СОИБ достигается путем:
  - инвестирования необходимых финансовых средств в обеспечение процессов СОИБ. При этом инвестирование не предполагает получение дохода от выполнения процессов СОИБ, а приводит к снижению предполагаемой величины возможного ущерба (финансового эквивалента возможных потерь) организации БС РФ в случае реализации актуальных для организации БС РФ рисков нарушения ИБ;
  - обеспечения необходимых и достаточных кадровых ресурсов. Рекомендации к определению потребностей службы ИБ организации БС РФ в обеспечении кадровыми ресурсами установлены в разделе 8 настоящего документа;

– проводить контроль эффективности инвестирования в обеспечение процессов СОИБ путем установления и мониторинга целевых (контрольных) показателей, выраженных в количественной (денежной) форме. Рекомендации к проведению контроля эффективности инвестирования в обеспечение процессов СОИБ установлены в разделе 9 настоящего документа.

6. Рекомендации к методологии оценивания уровня зрелости выполнения процессов СОИБ

6.1. С целью установления и применения методологии оценивания уровня зрелости выполнения процессов СОИБ организации БС РФ рекомендуется:
– установить состав процессов СОИБ, направленных на непосредственное обеспечение ИБ, уровень зрелости выполнения которых влияет на величину остаточных рисков нарушения ИБ организации БС РФ;
– установить показатели уровня зрелости выполнения процессов СОИБ организации БС РФ.

6.2. Организациям БС РФ рекомендуется установить в качестве процессов СОИБ, направленных на непосредственное обеспечение ИБ, уровень зрелости выполнения которых влияет на величину остаточных рисков нарушения ИБ организации БС РФ, среди прочих следующие.

6.2.1. Процессы СОИБ, реализуемые в соответствии с положениями, установленными в разделе 7 “Система информационной безопасности организаций банковской системы Российской Федерации” СТО БР ИББС-1.0:
– обеспечение ИБ при назначении и распределении ролей;
– обеспечение ИБ при эксплуатации и снятии с эксплуатации автоматизированных банковских систем (АБС), используемых для реализации банковских платежных и информационных технологических процессов;
– обеспечение ИБ при управлении доступом и регистрацией;
– обеспечение ИБ средствами антивирусной защиты;
– обеспечение ИБ при использовании ресурсов сети Интернет;
– обеспечение ИБ при использовании средств криптографической защиты информации.

При установлении процессов СОИБ, уровень зрелости выполнения которых влияет на величину остаточных рисков нарушения ИБ организации БС РФ, рекомендуется дополнительно рассматривать следующие процессы:
– предотвращение утечек информации, контентный контроль информационного обмена и передачи информации за пределы локальной вычислительной сети организации БС РФ, в том числе при использовании сети Интернет;
– контроль вывода информации на печать;
– обеспечение защиты от сетевых атак;
– обеспечение целостности вычислительной среды;
– обеспечение защиты информации технологическими мерами, в том числе при осуществлении переводов денежных средств;
– контроль резервного копирования информации и целостности резервных копий.

6.2.2. Процессы СОИБ, реализуемые в соответствии с положениями, установленными в разделе 8 “Система менеджмента информационной безопасности организаций банковской системы Российской Федерации” СТО БР ИББС-1.0:
– обнаружение и реагирование на инциденты ИБ;
– мониторинг ИБ;
– обеспечение непрерывности бизнеса и его восстановления после прерывания.

6.3. Организации БС РФ при установлении показателей уровня зрелости выполнения процессов СОИБ рекомендуется выполнить следующие мероприятия:
– установить состав процессов СМИБ, полнота и качество выполнения которых влияет на уровень зрелости выполнения управляемых процессов СОИБ;
– установить и применять общую модель полноты и качества выполнения процессов СМИБ;
– с использованием общей модели оценивать полноту и качество выполнения каждого из процессов СМИБ для каждого управляемого процесса СОИБ;
– установить и применять общие правила определения показателей уровня зрелости выполнения управляемых процессов СОИБ на основе соответствующих оценок полноты и качества выполнения процессов СМИБ.

6.4. В качестве процессов СМИБ, полнота и качество выполнения которых влияют на уровень зрелости выполнения управляемых процессов СОИБ, рекомендуется среди прочего рассматривать процессы, реа-

лизуемые в соответствии с положениями, установленными в разделе 8 “Система менеджмента информационной безопасности организаций банковской системы Российской Федерации” СТО БР ИББС-1.0:

– определение/коррекция области действия процесса СОИБ;
– планирование реализации процесса СОИБ;
– разработка/коррекция внутренних документов, регламентирующих выполнение процесса СОИБ;
– выполнение планов реализации процесса СОИБ с учетом выполнения положений по обеспечению ИБ на этапах создания АБС;
– реализация автоматизации выполнения процесса СОИБ;
– реализация программ по обучению и повышению осведомленности в области выполнения процесса СОИБ;
– реализация контроля выполнения процесса СОИБ;
– включение процесса СОИБ в область самооценки и аудита ИБ;
– анализ реализации и выполнения процесса СОИБ;
– инициирование своевременного совершенствования процесса СОИБ.

6.5. Общая модель полноты и качества выполнения процессов СМИБ может быть установлена следующим образом:

– “Нулевой уровень”. Полное отсутствие каких-либо процессов СМИБ.
– “Первый уровень”. Процессы СМИБ применяются бессистемно и (или) эпизодически.
– “Второй уровень”. Процессы СМИБ применяются на постоянной основе. Общие подходы (способы) применения процессов СМИБ в организации БС РФ не установлены. Выполнение процессов СМИБ осуществляется на усмотрение исполнителя.
– “Третий уровень”. Процессы СМИБ применяются на постоянной основе в соответствии с общими подходами (способами), установленными в организации БС РФ.
– “Четвертый уровень”. Процессы СМИБ применяются на постоянной основе в соответствии с общими подходами (способами), установленными в организации БС РФ. В организации БС РФ реализованы контроль, анализ и необходимое своевременное совершенствование процессов СМИБ.
– “Пятый уровень”. Процессы СМИБ применяются на постоянной основе в соответствии с общими подходами (способами), установленными в организации БС РФ. В организации БС РФ реализованы анализ и необходимое совершенствование процессов СМИБ. Процессы СМИБ основаны на лучших отечественных и международных практиках.

6.6. Организации БС РФ рекомендуется определить весовые коэффициенты $0 \le \alpha_i \le 1$, где $\sum_i \alpha_i = 1$, которые характеризуют степень влияния уровня полноты и качества выполнения отдельного процесса СМИБ (L_i) на уровень зрелости выполнения управляемого процесса СОИБ в целом (L). Уровень зрелости выполнения управляемого процесса СОИБ рекомендуется рассчитывать по следующей формуле: $L = \left[\sum_i \alpha_i \cdot L_i\right]$, где $[x]$ – операция округления числа x.

7. Рекомендации к методологии оценивания рисков нарушения ИБ с учетом данных о реализованном организацией БС РФ уровне зрелости выполнения процессов СОИБ

7.1. С целью установления и применения методологии оценивания рисков нарушения ИБ с учетом данных о реализованном в организации БС РФ уровне зрелости выполнения процессов СОИБ организации БС РФ рекомендуется:

– установить способы учета влияния реализованного организацией БС РФ уровня зрелости выполнения процессов СОИБ при проведении оценки рисков нарушения ИБ;
– оценивать риски нарушения ИБ с учетом данных о реализованном организацией БС РФ уровне зрелости выполнения процессов СОИБ.

7.2. Организации БС РФ при установлении способов учета влияния реализованного уровня зрелости выполнения процессов СОИБ при проведении оценки рисков нарушения ИБ рекомендуется учитывать уровень зрелости выполнения процессов СОИБ в обратной зависимости к степени возможности реализации угроз ИБ (далее – СВР угроз ИБ), оцениваемой в соответствии с методологией оценки рисков нарушения ИБ, установленной РС БР ИББС-2.2.

7.3. При реализации учета влияния реализованного уровня зрелости выполнения процессов СОИБ на риски нарушения ИБ рекомендуется:

– оценить актуальность угроз нарушения ИБ, установленных в модели угроз организации БС РФ;
– оценить СВР угроз ИБ на основе оценки уровня зрелости выполнения процессов СОИБ, реализуемых для защиты от конкретных угроз ИБ.

7.4. Для оценки актуальности угроз нарушения ИБ рекомендуется использовать следующую качественную шкалу:
– минимальная;
– средняя;
– высокая;
– критическая.

7.5. Оценку СВР угроз ИБ с учетом данных о реализованном в организации БС РФ уровне зрелости выполнения процессов СОИБ рекомендуется проводить с использованием методик количественных оценок, например, следующим образом:

Таблица 1. Способ оценивания СВР угроз ИБ

		Актуальность угроз нарушения ИБ			
		Минимальная	**Средняя**	**Высокая**	**Критическая**
Уровень зрелости выполнения процесса СОИБ (L)	5-й уровень	0,01	0,02	0,03	0,05
	4-й уровень	0,05	0,1	0,15	0,2
	3-й уровень	0,1	0,15	0,25	0,3
	2-й уровень	0,15	0,25	0,35	0,45
	1-й уровень	0,2	0,45	0,75	0,9
	0-й уровень	0,25	0,55	0,95	1

7.6. Оценивать риски рекомендуется в количественной (денежной) форме для всех защищаемых информационных активов с учетом полученных значений СВР угроз ИБ по методикам, применяемым в организации БС РФ.

7.7. Потребность организации БС РФ в финансовых средствах для обеспечения процесса СОИБ рекомендуется определять, проводя анализ агрегированных значений предполагаемых величин возможного ущерба (финансового эквивалента возможных потерь) организации БС РФ в результате потенциальной реализации рисков нарушения ИБ (рисковых событий). При этом агрегирование указанных значений рекомендуется осуществлять по каждому из процессов СОИБ.

7.8. Рассчитанный объем финансовых средств для обеспечения процесса СОИБ рекомендуется распределять между процессами СМИБ, полнота и качество выполнения которых влияют на уровень зрелости выполнения управляемого процесса СОИБ, с использованием следующего коэффициента:

$$\beta_i = \frac{\alpha_i \cdot (L_{max} - L_i)}{\sum_i \alpha_i \cdot (L_{max} - L_i)}$$, где L_{max} – максимальный уровень полноты и качества выполнения процессов СМИБ.

8. Рекомендации к определению потребностей службы ИБ организации БС РФ в обеспечении кадровыми ресурсами

8.1. Определение потребности службы ИБ организации БС РФ в кадровых ресурсах заключается в установлении необходимого и достаточного количества, а также требуемой компетенции работников службы ИБ, выполняемой на основе:
– анализа задач и функций, возложенных на службу ИБ организации БС РФ;
– уровня автоматизации процессов СОИБ и централизации управления средствами автоматизации;
– прогноза возможного расширения состава задач и функций службы ИБ в соответствии с планами совершенствования процессов СОИБ вследствие развития бизнес-процессов организации БС РФ, совершенствования процессов информатизации организации БС РФ, развития филиальной сети организации БС РФ.

8.2. При планировании (совершенствовании) процессов СОИБ следует обеспечить выделение ресурсов ИБ для эффективной реализации требований законодательства РФ, нормативных актов Банка России, требований к обеспечению ИБ, установленных организацией БС РФ.

8.3. Организации БС РФ рекомендуется обеспечить службу ИБ кадровыми ресурсами, необходимыми и достаточными для реализации целевого уровня полноты и качества выполнения процессов СМИБ для каждого управляемого процесса СОИБ.

8.4. Среди основных задач и функций службы ИБ рекомендуется рассматривать реализацию деятельности в рамках процессов СМИБ организации БС РФ, группируя выполняемые задачи и функции по следующим направлениям:

– направление “методология”;
– направление “реализация и сопровождение”;
– направление “контроль”;
– направление “криптографическая защита”.

Организации БС РФ рекомендуется обеспечить выделение отдельных кадровых ресурсов для каждого из указанных направлений.

8.5. Организации БС РФ рекомендуется установить состав задач и функций службы ИБ для каждого уровня полноты и качества выполнения процесса СМИБ, оценив при этом трудозатраты на их выполнение.

Рекомендуется разделение задач и функций, выполняемых в рамках процессов СМИБ на функции, связанные с установлением общих подходов (способов) выполнения процессов СМИБ, непосредственного выполнения процессов СМИБ, анализа и контроля выполнения процессов СМИБ.

8.6. Задачи и функции, связанные с установлением общих подходов (способов) выполнения и анализа выполнения процессов СМИБ, рекомендуется возлагать на работников службы ИБ, задействованных по направлению “методология”.

8.7. Задачи и функции, связанные с контролем выполнения процессов СМИБ, рекомендуется возлагать на работников службы ИБ, задействованных по направлению “контроль”, или работников иных подразделений организации БС РФ, выполняющих функции по направлению внутреннего контроля.

8.8. Задачи и функции, связанные с непосредственным выполнением процессов СМИБ, рекомендуется разделять в соответствии со следующими общими правилами:

8.8.1. На работников службы ИБ, задействованных по направлению “методология”, рекомендуется возлагать непосредственное выполнение следующих процессов СМИБ:

– определение/коррекция области действия процесса СОИБ;
– планирование реализации процесса СОИБ;
– разработка/коррекция внутренних документов, регламентирующих выполнение процесса СОИБ;
– анализ реализации и выполнения процесса СОИБ;
– инициирование и подготовка программ по обучению и повышению осведомленности в области выполнения процесса СОИБ;
– инициирование своевременного совершенствования процесса СОИБ.

8.8.2. На работников службы ИБ, задействованных по направлению “реализация и сопровождение”, рекомендуется возлагать непосредственное выполнение следующих процессов СМИБ:

– сопровождение выполнения планов реализации процесса СОИБ с учетом выполнения положений по обеспечению ИБ на этапах создания АБС;
– сопровождение реализации автоматизации выполнения процесса СОИБ;
– сопровождение реализации программ по обучению и повышению осведомленности в области выполнения процесса СОИБ.

8.8.3. На работников службы ИБ, задействованных по направлению “контроль”, рекомендуется возлагать непосредственное выполнение следующих процессов СМИБ:

– реализация контроля области действия процесса СОИБ;
– реализация контроля выполнения процесса СОИБ;
– включение процесса СОИБ в область самооценки ИБ и аудита ИБ.

8.9. Потребность в кадровых ресурсах по направлению “криптографическая защита” определяется в соответствии с требованиями законодательства РФ, а также в соответствии с эксплуатационной документацией на используемые средства криптографической защиты информации.

8.10. Организациям БС РФ рекомендуется определить минимальную необходимую и достаточную численность работников службы ИБ исходя из следующих рекомендуемых показателей:

– трудозатраты на выполнение задачи и функций обеспечения ИБ;
– количество реализуемых процессов СОИБ;
– масштаб выполнения управляемого процессов СОИБ, в том числе:
  - количество подразделений (филиалов, отделений) организации БС РФ;
  - количество АБС;
  - количество работников организации БС РФ;
  - территориальное расположение подразделений организации БС РФ.

Численность работников службы ИБ рекомендуется определять для каждого филиала организации БС РФ.

8.11. Работники службы ИБ должны обладать компетенцией, необходимой для выполнения их функциональных обязанностей. Определение компетенции сводится к установлению требований в отношении знаний, практических навыков и опыта работы в соответствующей области работников службы ИБ.

К основным требованиям, определяющим необходимую компетенцию работников службы ИБ, следует среди прочего относить:

– наличие высшего профессионального образования в области ИБ и (или) информационных технологий;
– опыт работы в области ИБ не менее определенного периода, например не менее трех лет;
– регулярное прохождение дополнительного (специализированного) обучения (повышения квалификации) в области ИБ;
– знание требований законодательства РФ, в том числе нормативных актов Банка России, необходимых для надлежащего выполнения функций, возложенных на работников службы ИБ;
– знание внутренних нормативно-методических и организационно-распорядительных документов организации БС РФ в области ИБ;
– осведомленность по вопросам, касающимся средств, систем и технологий обеспечения ИБ, а также способов и практик их применения.

9. Рекомендации к проведению контроля эффективности инвестирования в обеспечение процессов СОИБ

9.1. Достижение надлежащего баланса между величинами рисков нарушения ИБ, связанных с наличием уязвимостей при выполнении процессов СОИБ, и ресурсным обеспечением ИБ, направленным на снижение указанных рисков путем обеспечения необходимого и достаточного уровня зрелости выполнения процессов СОИБ, рекомендуется обеспечивать путем определения и анализа целевых (контрольных) показателей эффективности использования финансовых средств, инвестированных в повышение уровня зрелости выполнения процессов СОИБ.

9.2. Показатели эффективности рекомендуется разделять на две группы:

– показатели, подлежащие анализу на этапе планирования инвестирования в повышение уровня зрелости выполнения процессов СОИБ;
– показатели, подлежащие анализу на этапе оценки результатов инвестирования в уровень зрелости выполнения процессов СОИБ.

9.3. В качестве основных показателей эффективности инвестирования в выполнение процессов СОИБ на этапе планирования рекомендуется рассматривать:

– ожидаемые результаты от снижения уровня рисков нарушения ИБ, связанных с повышением уровня зрелости выполнения процессов СОИБ;
– срок получения ожидаемых результатов по повышению уровня зрелости выполнения процессов СОИБ;
– согласованность со стратегией ИТ-развития организации БС РФ.

Указанные показатели эффективности рекомендуется оценивать экспертным путем с привлечением профильных подразделений организации БС РФ и включать в оценку финансовых средств, инвестированных в повышение уровня зрелости выполнения процессов СОИБ.

9.4. В качестве основного показателя эффективности инвестирования финансовых средств в повышение уровня зрелости выполнения процессов СОИБ на этапе оценки результатов инвестирования рекомендуется рассматривать соотношение фактического ущерба (финансового эквивалента понесенных потерь) от инцидентов ИБ, в том числе непосредственных финансовых потерь от инцидентов ИБ, финансовых потерь от нарушения непрерывности деятельности организации БС РФ, финансовых потерь от негативного влияния инцидентов ИБ на деловую репутацию, финансовые средства, затраченные для ликвидации последствий инцидентов ИБ, по отношению к предполагаемой на этапе планирования величине возможного ущерба (финансового эквивалента возможных потерь) организации БС РФ.

9.5. При превышении фактических финансовых потерь от инцидентов ИБ значений, предполагаемых на этапе планирования, организации БС РФ рекомендуется определить основные факторы возникновения рисковых событий, приводящих к ущербу (финансовым потерям) и выработать планы, элементами которых могут являться:

– пересмотр модели угроз и нарушителя, применяемых требований к обеспечению ИБ;
– установление новых процессов СОИБ, в том числе связанных с изменениями состава актуальных угроз;
– повышение уровня зрелости выполнения установленных процессов СОИБ.

9.6. В качестве дополнительного показателя эффективности инвестирования в повышение уровня зрелости выполнения процессов СОИБ на этапе оценки результатов инвестирования рекомендуется рассматривать соответствие фактических сроков реализации планов по повышению уровня зрелости выполнения процессов СОИБ планируемым срокам.

9.7. Организации БС РФ рекомендуется выполнять с установленной периодичностью:

– анализ эффективности выполнения процессов СОИБ, в том числе выполняемый на основе показателей, установленных в пункте 9.2 настоящего документа;
– анализ рисков нарушения ИБ с целью определения приоритетных направлений совершенствования процессов СОИБ.

Периодичность проведения анализа рекомендуется согласовывать с планами реализации или повышения уровня зрелости выполнения процессов СОИБ.

Приложение А
(справочное)

Пример расчета ресурсов ИБ организации БС РФ

1. Общие положения

1.1. В настоящем примере приведен расчет ресурсов ИБ организации БС РФ в части:

обеспечения процесса управления доступом и регистрацией (подконтрольный процесс) финансовыми средствами;

обеспечения службы ИБ организации БС РФ кадровыми ресурсами, необходимыми и достаточными для обеспечения всех процессов СОИБ организации БС РФ, направленных на непосредственное обеспечение ИБ.

1.2. В рамках данного примера при расчете обеспечения подконтрольного процесса финансовыми средствами предполагается, что организацией БС РФ определена степень тяжести последствий от реализации угроз ИБ, связанных с несанкционированным доступом, выраженная в количественной (денежной) форме, величина которой составляет P.

Целевое значение СВР угроз ИБ составляет величину $p_{пр} = 0,05$. Допустимым остаточным риском организацией БС РФ принята величина $p_{пр} \cdot P$.

При этом актуальность угрозы утечки защищаемой информации в результате несанкционированного доступа оценивается организацией БС РФ как средняя.

1.3. В рамках данного примера при расчете обеспечения службы ИБ организации БС РФ кадровыми ресурсами предполагается, что:

число ключевых АБС, эксплуатируемых в организации БС РФ, составляет 15;

число процессов СОИБ составляет 9;

число работников, отделений и расстояний между отделениями разное для филиалов;

коэффициент невыхода работников организации БС РФ составляет 1,1.

2. Расчет уровня зрелости выполнения подконтрольного процесса

2.1. Определение процессов СМИБ, полнота и качество выполнения которых влияет на уровень зрелости выполнения подконтрольного процесса.

Процессу управления доступом и регистрацией соответствуют следующие процессы СМИБ:

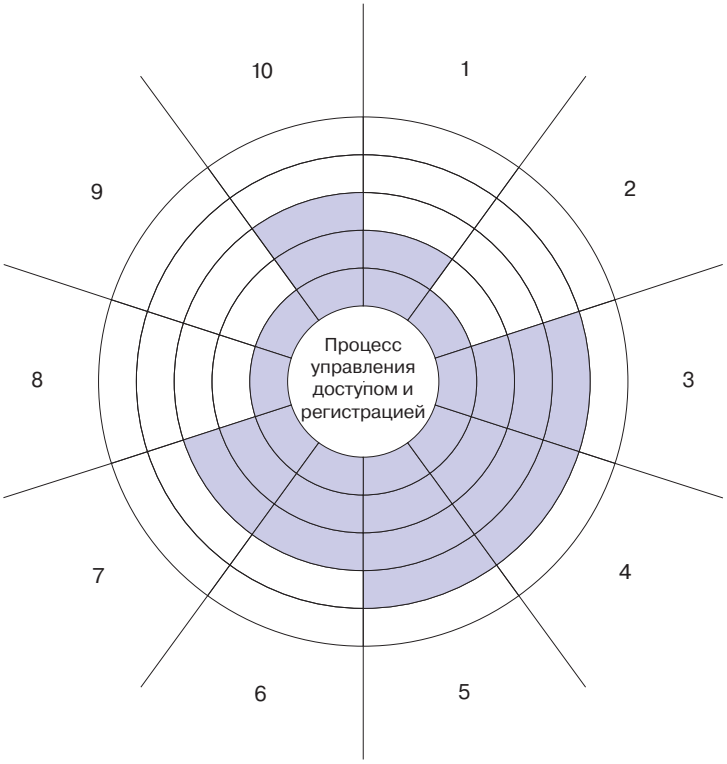
- определение/коррекция области действия подконтрольного процесса;
- планирование реализации подконтрольного процесса;
- разработка/коррекция внутренних документов, регламентирующих выполнение подконтрольного процесса;
- выполнение планов реализации подконтрольного процесса с учетом выполнения положений по обеспечению ИБ на этапах создания АБС;
- реализация автоматизации выполнения подконтрольного процесса;
- реализация программ по обучению и повышению осведомленности в области выполнения подконтрольного процесса;
- реализация контроля выполнения подконтрольного процесса;
- включение подконтрольного процесса в область самооценки и аудита ИБ;
- анализ реализации и выполнения подконтрольного процесса;
- инициирование своевременного совершенствования подконтрольного процесса.

2.2. Оценка уровней полноты и качества выполнения процессов СМИБ, влияющих на уровень зрелости выполнения подконтрольного процесса.

№ п/п	Процесс СМИБ	Качественная оценка	Весовой коэффициент	Уровень зрелости
1	Определение/коррекция области действия подконтрольного процесса	Определение/коррекция области действия подконтрольного процесса применяется на постоянной основе. Общие подходы (способы) определения/коррекции области действия подконтрольного процесса не установлены. Определение/коррекция области действия подконтрольного процесса осуществляется по усмотрению исполнителя	0,1	2

№ п/п	Процесс СМИБ	Качественная оценка	Весовой коэффициент	Уровень зрелости
2	Планирование реализации подконтрольного процесса	Планирование реализации подконтрольного процесса применяется бессистемно и (или) эпизодически	0,05	1
3	Разработка/коррекция внутренних документов, регламентирующих выполнение подконтрольного процесса	Разработка/коррекция внутренних документов, регламентирующих выполнение подконтрольного процесса, осуществляется на постоянной основе в соответствии с общими подходами (способами), установленными в организации БС РФ. В организации БС РФ реализованы контроль, анализ и необходимое своевременное совершенствование процессов разработки/коррекции внутренних документов, регламентирующих выполнение подконтрольного процесса	0,2	4
4	Выполнение планов реализации подконтрольного процесса с учетом выполнения положений по обеспечению ИБ на этапах создания АБС	Выполнение планов реализации подконтрольного процесса с учетом выполнения положений по обеспечению ИБ на этапах создания АБС осуществляется на постоянной основе в соответствии с общими подходами (способами), установленными в организации БС РФ. В организации БС РФ реализованы контроль, анализ и необходимое своевременное совершенствование планов реализации подконтрольного процесса с учетом выполнения положений по обеспечению ИБ на этапах создания АБС	0,05	4
5	Реализация автоматизации выполнения подконтрольного процесса	Автоматизация выполнения подконтрольного процесса осуществляется на постоянной основе в соответствии с общими подходами (способами), установленными в организации БС РФ. В организации БС РФ реализованы контроль, анализ и необходимое своевременное совершенствование процессов автоматизации выполнения подконтрольного процесса	0,25	4
6	Реализация программ по обучению и повышению осведомленности в области выполнения подконтрольного процесса	Реализация программ по обучению и повышению осведомленности в области выполнения подконтрольного процесса осуществляется на постоянной основе в соответствии с общими подходами (способами), установленными в организации БС РФ	0,05	3
7	Реализация контроля выполнения подконтрольного процесса	Реализация контроля выполнения подконтрольного процесса осуществляется на постоянной основе в соответствии с общими подходами (способами), установленными в организации БС РФ	0,15	3
8	Включение подконтрольного процесса в область самооценки и аудита ИБ	Включение подконтрольного процесса в область самооценки и аудита ИБ осуществляется бессистемно и (или) эпизодически	0,05	1
9	Анализ реализации и выполнения подконтрольного процесса	Анализ реализации и выполнения подконтрольного процесса осуществляется бессистемно и (или) эпизодически	0,05	1
10	Инициирование своевременного совершенствования подконтрольного процесса	Инициирование своевременного совершенствования подконтрольного процесса осуществляется на постоянной основе в соответствии с общими подходами (способами), установленными в организации БС РФ	0,05	3

2.3. Определение уровня зрелости выполнения подконтрольного процесса.



Выполнение процесса управления доступом и регистрацией имеет уровень зрелости

$$L = \left[\sum_i \alpha_i \cdot L_i\right] = [0{,}1 \cdot 2 + 0{,}05 \cdot 1 + 0{,}2 \cdot 4 + 0{,}05 \cdot 4 + 0{,}25 \cdot 4 + 0{,}05 \cdot 3 + 0{,}15 \cdot 3 + 0{,}05 \cdot 1 + 0{,}05 \cdot 1 + 0{,}05 \cdot 1] = 3.$$

3. Оценка степени вероятности угроз ИБ с учетом данных о реализованном в организации БС РФ уровне зрелости выполнения процессов СОИБ

		Актуальность угроз утечки защищаемой информации в результате несанкционированного доступа			
		Минимальная	**Средняя**	**Высокая**	**Критическая**
Уровень зрелости выполнения подконтрольного процесса	5-й уровень	0,01	0,02	0,03	0,05
	4-й уровень	0,05	0,1	0,15	0,2
	3-й уровень	0,1	0,15	0,25	0,3
	2-й уровень	0,15	0,25	0,35	0,45
	1-й уровень	0,2	0,45	0,75	0,9
	0-й уровень	0,25	0,55	0,95	1

Вычисленная величина СВР угроз ИБ ($p_{свр}$) равна значению 0,15, что превышает целевое значение $p_{пр} = 0{,}05$.

Риск нарушения ИБ, связанный с возможной утечкой защищаемой информации в результате несанкционированного доступа, выше приемлемого остаточного риска.

4. Расчет финансовых средств, которые могут быть затрачены организацией БС РФ на повышение уровня зрелости выполнения подконтрольного процесса

Финансовые средства, которые могут быть затрачены организацией БС РФ на повышение уровня ИБ процесса управления доступом и регистрацией, не должны превышать величину $C = P \cdot (p_{свр} - p_{пр}) = 0{,}1 \cdot P$, при этом финансовые средства, которые могут быть затрачены организацией БС РФ на повышение уровня полноты и качества соответствующих процессов СМИБ процесса управления доступом и регистрацией, могут быть оценены следующим образом:

№ п/п	Процесс СМИБ	Весовой коэффициент	Оценка финансовых средств
1	Определение/коррекция области действия подконтрольного процесса	0,1	$C \cdot \frac{\alpha_i \cdot (5 - L_i)}{\sum_i \alpha_i \cdot (5 - L_i)} = C \cdot \frac{3}{19}$
2	Планирование реализации подконтрольного процесса	0,05	$C \cdot \frac{\alpha_i \cdot (5 - L_i)}{\sum_i \alpha_i \cdot (5 - L_i)} = C \cdot \frac{2}{19}$
3	Разработка/коррекция внутренних документов, регламентирующих выполнение подконтрольного процесса	0,2	$C \cdot \frac{\alpha_i \cdot (5 - L_i)}{\sum_i \alpha_i \cdot (5 - L_i)} = C \cdot \frac{2}{19}$
4	Выполнение планов реализации подконтрольного процесса с учетом выполнения положений по обеспечению ИБ на этапах создания АБС	0,05	$C \cdot \frac{\alpha_i \cdot (5 - L_i)}{\sum_i \alpha_i \cdot (5 - L_i)} = C \cdot \frac{1}{38}$
5	Реализация автоматизации выполнения подконтрольного процесса	0,25	$C \cdot \frac{\alpha_i \cdot (5 - L_i)}{\sum_i \alpha_i \cdot (5 - L_i)} = C \cdot \frac{5}{38}$
6	Реализация программ по обучению и повышению осведомленности в области выполнения подконтрольного процесса	0,05	$C \cdot \frac{\alpha_i \cdot (5 - L_i)}{\sum_i \alpha_i \cdot (5 - L_i)} = C \cdot \frac{1}{19}$
7	Реализация контроля выполнения подконтрольного процесса	0,15	$C \cdot \frac{\alpha_i \cdot (5 - L_i)}{\sum_i \alpha_i \cdot (5 - L_i)} = C \cdot \frac{3}{19}$
8	Включение подконтрольного процесса в область самооценки и аудита ИБ	0,05	$C \cdot \frac{\alpha_i \cdot (5 - L_i)}{\sum_i \alpha_i \cdot (5 - L_i)} = C \cdot \frac{2}{19}$
9	Анализ реализации и выполнения подконтрольного процесса	0,05	$C \cdot \frac{\alpha_i \cdot (5 - L_i)}{\sum_i \alpha_i \cdot (5 - L_i)} = C \cdot \frac{2}{19}$
10	Инициирование своевременного совершенствования подконтрольного процесса	0,05	$C \cdot \frac{\alpha_i \cdot (5 - L_i)}{\sum_i \alpha_i \cdot (5 - L_i)} = C \cdot \frac{1}{19}$

5. Расчет кадровых ресурсов, необходимых для повышения уровня зрелости выполнения процессов СОИБ и позволяющих свести риск нарушения ИБ до приемлемого уровня

5.1. Головное подразделение организации БС РФ:

Направление "методология":

Функция по обеспечению ИБ	Трудоемкость[1], часов в год
установление общих подходов (способов) выполнения и анализа выполнения процессов СМИБ (регламентация процессов СМИБ)	100 для каждого процесса СМИБ, всего 1000
определение/коррекция области действия каждого процесса СОИБ	100 для каждого процесса СОИБ, всего 900
планирование реализации процесса СОИБ	60 для каждого процесса СОИБ, всего 540
разработка/коррекция внутренних документов, регламентирующих выполнение процесса СОИБ	200 для каждого процесса СОИБ, всего 1800
анализ реализации и выполнения процесса СОИБ	60 для каждого процесса СОИБ, всего 540
инициирование и подготовка программ по обучению и повышению осведомленности в области выполнения процесса СОИБ	20 для каждого процесса СОИБ, всего 180
инициирование своевременного совершенствования процесса СОИБ	60 для каждого процесса СОИБ, всего 540
	Всего по направлению с учетом коэффициента невыхода: 6050 – 3 человека

Направление "реализация и сопровождение":

Функция по обеспечению ИБ	Трудоемкость, часов в год
сопровождение выполнения планов реализации процесса СОИБ с учетом выполнения положений по обеспечению ИБ на этапах создания АБС	75 для каждого процесса СОИБ, 75 для каждой АБС, всего 1800
сопровождение реализации автоматизации выполнения процессов СОИБ	100 для каждого процесса СОИБ, 100 для каждой АБС, всего 4800
сопровождение реализации программ по обучению и повышению осведомленности в области выполнения процессов СОИБ	30 для каждого процесса СОИБ, всего 270
	Всего по направлению с учетом коэффициента невыхода: 7557 – 4 человека

Направление "контроль":

Функция по обеспечению ИБ	Трудоемкость, часов в год
контроль выполнения процессов СМИБ	250 для каждого процесса СМИБ, всего 2500
организация контроля области действия процесса СОИБ	50 для каждого процесса СОИБ, всего 450
включение процесса СОИБ в область самооценки ИБ и аудита ИБ	50 для каждого процесса СОИБ, всего 450
	Всего по направлению с учетом коэффициента невыхода: 3740 – 2 человека

Направление "криптографическая защита":

По направлению "криптографическая защита" в соответствии с эксплуатационной документацией на используемые средства криптографической защиты информации требуется наличие двух работников.

[1] Трудоемкость определяется экспертно организацией БС РФ на основе опыта реализации процессов СОИБ и квалификации работников.

5.2. Филиал организации БС РФ:

Для филиалов организации БС РФ рассчитывается минимальная необходимая численность службы ИБ, после чего для подсчета численности службы ИБ конкретного филиала используются уточняющие коэффициенты.

Направление "методология":

Функция по обеспечению ИБ	Трудоемкость, часов в год
уточнение (адаптация) общих подходов (способов) выполнения и анализа выполнения процессов СМИБ (регламентация процессов СМИБ)	350
уточнение области действия каждого процесса СОИБ	350
планирование реализации процесса СОИБ	350
уточнение (адаптация) внутренних документов, регламентирующих выполнение процесса СОИБ	350
анализ реализации и выполнения процесса СОИБ	200
участие в подготовке программ по обучению и повышению осведомленности в области выполнения процесса СОИБ	200
инициирование своевременного совершенствования процесса СОИБ	200
	Всего по направлению с учетом коэффициента невыхода: 2200 – 1 человек

Минимальная необходимая численность службы ИБ филиала по направлению "методология" составляет 1 человек, для расчета численности службы ИБ конкретного филиала по направлению "методология" используется следующая формула:

$$H_1 = \max\left(1, \left[\frac{н_п}{H_п}\right]\right),$$

где:

$н_п$ – количество отделений в филиале;

$H_п$ – среднее количество отделений на один филиал;

[ ] – операция округления;

max(*a*,*b*) – операция "максимальное из двух чисел *a* и *b*".

Направление "реализация и сопровождение":

Функция по обеспечению ИБ	Трудоемкость, часов в год
участие в выполнении планов реализации процесса СОИБ с учетом выполнения положений по обеспечению ИБ на этапах создания АБС	25 для каждого процесса СОИБ, 25 для каждой АБС, всего 600
участие в реализации автоматизации выполнения процессов СОИБ	100 для каждого процесса СОИБ, всего 900
участие в реализации программ по обучению и повышению осведомленности в области выполнения процессов СОИБ	200
	Всего по направлению с учетом коэффициента невыхода: 1870 – 1 человек

Минимальная необходимая численность службы ИБ филиала по направлению "сопровождение" составляет 1 человек, для расчета численности службы ИБ конкретного филиала по направлению "сопровождение" используется следующая формула:

$$H_2 = \max\left(1, \left[\frac{н_р}{H_р}\right]\right),$$

где:
$н_п$ – количество работников в филиале;
$Н_п$ – среднее количество работников на один филиал;
[ ] – операция округления;
max(*a*,*b*) – операция “максимальное из двух чисел *a* и *b*”.

Направление “контроль”:

Функция по обеспечению ИБ	Трудоемкость, часов в год
участие в контроле выполнения процессов СМИБ	50 для каждого процесса СОИБ, 25 для каждой АБС, всего 750 часов
организация контроля области действия процесса СОИБ	350
участие в проведении самооценки ИБ и аудита ИБ	450
	Всего по направлению с учетом коэффициента невыхода: 1705 – 1 человек

Минимальная необходимая численность службы ИБ филиала по направлению “контроль” составляет 1 человек, для расчета численности службы ИБ конкретного филиала по направлению “контроль” используется следующая формула:

$$H_з = \max\left(1, \left[\frac{н_п}{Н_п}\right], \left[\frac{н_р}{Н_р}\right], \left[\frac{н_{раст}}{Н_{раст}}\right]\right) + (N_з - 1),$$

где:
$н_п$ – количество отделений в филиале;
$Н_п$ – среднее количество отделений на один филиал;
$н_р$ – количество работников в филиале;
$Н_р$ – среднее количество работников на один филиал;
$н_{раст}$ – среднее расстояние от отделения до филиала по филиалу;
$Н_{раст}$ – среднее расстояние от отделения до филиала по организации БС РФ;
$N_з$ – число зданий в филиале (без учета отделений);
[ ] – операция округления;
max(*a*,*b*,*c*,*d*) – операция “максимальное из четырех чисел *a*, *b*, *c*, *d*”.
5.3. Окончательный расчет:
Численность службы ИБ головного подразделения организации БС РФ – 11 человек.
Минимальная численность службы ИБ филиала – 3 человека.
Численность службы ИБ конкретного филиала вычисляется по формуле:
$H = H_1 + H_2 + H_3$.

Ключевые слова: банковская система Российской Федерации, система обеспечения информационной безопасности, система менеджмента информационной безопасности, служба информационной безопасности, ресурсное обеспечение информационной безопасности.