ФБК
Grant Thornton

Новые требования Банка России по управлению операционным риском в кредитных организациях

Москва | Июль 2020

Программа вебинара

Тема

Положение Банка России №716-П: новые вызовы и новые возможности в управление операционным риском

- Операционный риск как совокупность множества рисков
- Процедуры управления операционным риском: требования регулятора и обязанности кредитных организаций
- База событий операционного риска – главный инструмент знаний о операционном риске
- Классификатор событий операционного риска: унификация и регламентация

Спикер

Савицкая Майя

Менеджер

Департамент аудиторских и консультационных услуг финансовым институтам

ФБК Grant Thornton

ФБК
Grant Thornton

Программа вебинара

Тема

Управления риском информационных безопасности: новые требования и важные нюансы

- «Новые» обязанности служб информационной безопасности (ИБ).
- Порядок управления риском ИБ.
- Система внутренних документов и основные мероприятия по управлению риском ИБ и киберриском.
- Отчетность по рискам информационной безопасности.
-

Спикер

Черненко Александр

Директор
FBK | Cybersecurity

ФБК
Grant Thornton

Программа вебинара

Тема

Обзор Положения БР №716-П в части управления риском информационных систем

- Документирование положений по управлению риском информационных систем как обязанность кредитной организации;
- Разработка Политики информационных систем с учетом требований Банка России;
- Определение требований к информационным системам с учетом их влияния на обеспечение бесперебойной работы процессов кредитной организации;
- Основные положения обеспечения непрерывности и качества функционирования информационных систем;
- Обязанности и отчетность лиц, ответственных за риски информационных систем.

Спикер

Карпушкин Алексей

Ведущий эксперт, руководитель направления по ИТ-аудиту

Департамент аудиторских и консультационных услуг финансовым институтам

ФБК Grant Thornton

ФБК
Grant Thornton

Положение Банка России №716-П: новые вызовы и новые возможности в управление операционным риском

Савицкая Майя

Менеджер

Департамент аудиторских и консультационных услуг финансовым институтам ФБК Grant Thornton

ФБК
Grant Thornton

ВВЕДЕНИЕ

Положения Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

Вступает в силу с 1 октября 2020 года.

Система управления операционным риском подлежит приведению в соответствие с требованиями Положения №716-П кредитными организациями (головными кредитными организациями банковской группы) (далее – «КО»), в срок до 1 января 2022 года.

КО в случае приведения системы управления операционным риском в соответствие с требованиями Положения №716-П ранее 1 января 2022 года, вправе проинформировать об этом Банк России в целях организации Банком России оценки соответствия системы управления операционным риском требованиям Положения.

Разным банкам – разные требования

Банк, размер активов которого составляет 500 миллиардов рублей и более на начало текущего отчетного года

Банк с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей на начало текущего отчетного года

Кредитная организация (головная кредитная организация банковской группы), которая на начало текущего отчетного года является банком с базовой лицензией

Кредитная организация (головная кредитная организация банковской группы), которая на начало текущего отчетного года является небанковской кредитной организацией

Что такое операционный риск?

“

Пункт 4.1 приложения 1
к Указанию Банка России от 15.04.2015 № 3624-У
«О требованиях к системе управления рисками и капиталом кредитной организации и банковской группы»

”

Понятие операционного риска

Было

Риск **возникновения убытков** в результате ненадежности и недостатков внутренних процедур управления кредитной организации, отказа информационных и иных систем либо вследствие влияния на деятельность кредитной организации внешних событий.

Правовой риск является частью операционного риска.

Стало

Риск **возникновения прямых и непрямых потерь** в результате несовершенства или ошибочных внутренних процессов кредитной организации, действий персонала и иных лиц, сбоев и недостатков информационных, технологических и иных систем, а также в результате реализации внешних событий.

Правовой риск, риск информационной безопасности (включая киберриск) и риск информационных систем являются частью операционного риска.

Виды операционного риска

1. Риск информационной безопасности
2. Риск информационных систем
3. Правовой риск
4. Риск ошибок в управлении проектами
5. Риск ошибок в управленческих процессах
6. Риск ошибок в процессах осуществления внутреннего контроля
7. Модельный риск
8. Риск потерь средств клиентов, контрагентов, работников и третьих лиц (не компенсированных кредитной организацией)
9. Риск ошибок процесса управления персоналом
10. Риск платежной системы

ФБК
Grant Thornton

СИСТЕМА УПРАВЛЕНИЯ ОПЕРАЦИОННЫМ РИСКОМ

Элементы системы управления ОР

- ✓ **процедуры управления операционным риском;**
- ✓ **классификатор событий операционного риска;**
- ✓ **база событий ОР;**
- ✓ **контрольные показатели уровня операционного риска;**
- ✓ подразделение КО, ответственное за организацию управления операционным риском, структурно входящее в службу управления рисками КО;
- ✓ специализированные подразделения КО, которые в рамках функциональных обязанностей выполняют процедуры управления операционным риском, в части отдельных видов операционного риска;
- ✓ подразделение КО, уполномоченное проводить ежегодную оценку эффективности функционирования системы управления ОР риском. Такое подразделение должно быть структурно независимым от службы управления рисками (например, служба внутреннего аудита);
- ✓ автоматизированная информационная система, обеспечивающая функционирование как в целом системы управления операционным риском, так и отдельных ее элементов (например, базы событий), в том числе сохранность данных и их защиту от искажений;
- ✓ дополнительные элементы системы управления операционным риском, определенные в соответствии с главой 4 Положения 716-П.

ПРОЦЕДУРЫ УПРАВЛЕНИЯ ОПЕРАЦИОННЫМ РИСКОМ

Пункт 4.1 приложения 1

к Указанию Банка России от 15.04.2015 года № 3624-У

Процедуры по управлению операционным риском должны предусматривать:

- полномочия руководителей структурных подразделений кредитной организации в области управления операционным риском и их ответственность за выявление и оценку операционного риска, присущего деятельности этих подразделений;

- наличие в кредитной организации подразделения (работников), осуществляющего разработку процедур по управлению операционным риском, включая методы оценки операционного риска, и составление отчетов об операционном риске, а также применение указанных процедур;

- осуществление контроля за выполнением принятых в кредитной организации процедур по управлению операционным риском и оценки их эффективности службой внутреннего аудита кредитной организации (иным подразделением кредитной организации, независимым от подразделений, осуществляющих операции (сделки), связанные с принятием рисков, разработкой и применением процедур по управлению операционным риском);

- **иные процедуры, установленные пунктом 2.1 Положения БР N 716-П.**

1. Идентификация операционного риска

- ✓ анализ базы событий;
- ✓ проведение подразделениями ежегодной самооценки уровня операционного риска
- ✓ анализ динамики количественных показателей, направленных на измерение и контроль уровня операционного риска в определенный момент времени (ключевых индикаторов риска – КИР));
- ✓ интервью с работниками КО;
- ✓ анализ актов проверок, судебных актов (решений, определений, постановлений) и (или) актов исполнительных органов государственной власти, Банка России в части фактов, относящихся к реализации операционного риска;
- ✓ анализ информации уполномоченного подразделения и внешнего аудита;
- ✓ анализ информации работников, полученной в рамках инициативного информирования работниками КО службы управления рисками и (или) службы внутреннего аудита;
- ✓ анализ других внешних и внутренних источников информации и способов выявления рисков.

2. Сбор и регистрация информации о внутренних событиях ОР и потерях от его реализации

- ✓ автоматизированное выявление информации из информационных систем о реализовавшихся или возможных в будущем событиях ОР;
- ✓ неавтоматизированное выявление и сбор информации о событиях ОР, предусматривающие с использованием экспертного мнения выявление информации и проведение анализа обстоятельств и причин произошедших событий ОР , в случае, если автоматизированное выявление и сбор информации о событиях операционного риска невозможны.;
- ✓ ввод информации о событиях операционного риска в базу событий по алгоритмизированным правилам, установленным КО в ВНД;
- ✓ классификацию выявленных событий ОР
- ✓ определение потерь от реализации событий ОР
- ✓ регистрацию событий операционного риска в базе событий; определение стоимости возмещений потерь от реализации событий ОР в базе событий;
- ✓ обновление информации о событиях операционного риска в базе событий при выяснении новых обстоятельств их реализации;
- ✓ актуализацию источников информации о событиях ОР и сведений о центрах компетенций, ответственных за их сбор.

3. Определение потерь и возмещений потерь от реализации событий операционного риска

- ✓ учет потерь КО, включая установление сроков выявления и правил отражения в бухгалтерском учете;
- ✓ порядок и методы определения потерь КО от события операционного риска;
- ✓ порядок выявления расходов, относящихся к ОР, из общих КО, в том числе порядок выявления и сверки событий ОР с данными бухгалтерского учета;
- ✓ порядок и методы оценки недополученных доходов, связанных с событиями ОР;
- ✓ порядок и методы определения потенциальных потерь;
- ✓ порядок и методы определения стоимости возмещений от событий ОР;
- ✓ отбор и назначение экспертов КО, ответственных за расчет потерь от реализации событий ОР.

4.Количественная оценка уровня операционного риска

Способы проведения

- ✓ агрегированная оценка уровня операционного риска по КО;
- ✓ оценка объема капитала, выделяемого КО в рамках ВПОДК на покрытие потерь от реализации событий ОР;
- ✓ оценка ожидаемых потерь от реализации ОР.

Важно: *оценка ведется в целом по кредитной организации (головной кредитной организации банковской группы), в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов*

5.Качественная оценка уровня операционного риска

Способы проведения

- ✓ самооценка ОР (не реже одного раза в год)
- ✓ профессиональная оценка выделенными для данной процедуры работниками подразделений КО и (или) внешними экспертами;
- ✓ сценарный анализ операционных рисков.

Важно: *качественная оценка ОР проводится на основе ежегодного «Плана проведения качественной оценки», утверждаемого коллегиальным исполнительным органом КО.*

6. Выбор и применение способа реагирования на операционный риск

- **уклонение от риска** - отказ КО от оказания соответствующего вида услуг и операций в связи с высоким уровнем операционного риска в них;
- **передача риска** - страхование, передача риска другой стороне - контрагенту и (или) клиенту;
- **принятие риска** - готовность КО принять возможные потери в рамках установленного лимита потерь с процедурой контроля соблюдения лимита;
- принятие мер, направленных на уменьшение негативного влияния ОР на качество процессов, величины валовых потери от реализации ОР - **разработка форм (способов) контроля**, которые включают:

✓ изменения, вносимые в процессы;

✓ установление дополнительных форм (способов) контроля;

✓ обучение работников, в том числе участников процессов;

✓ применение автоматизированных решений.

Важно: *применение способов реагирования ни риск необходимо начинать в срок не более трех месяцев со дня проведения оценки уровня операционного риска*

ФБК
Grant Thornton

7. Мониторинг операционного риска

- ✓ установление и мониторинг КИР;
- ✓ анализ статистики событий ОР, в том числе причин возникновения событий операционного риска и потерь от их реализации;
- ✓ контроль выполнения мероприятий, направленных на повышение качества системы управления ОР и уменьшение его негативного влияния, включая мероприятия, направленные на предотвращение (снижение вероятности) событий ОР
- ✓ контроль выполнения мер, направленных на уменьшение негативного влияния ОР;
- ✓ контроль соблюдения выбранных способов реагирования на ОР;
- ✓ мониторинг потоков информации в рамках реализации ОР, поступающей от подразделений КО и центров компетенций, единоличного и коллегиального органов управления КО, из других источников информации.

Ключевые индикаторы риска (КИР)

Количественные показатели, направленные на измерение и контроль уровня операционного риска в определенный момент времени

ФБК
Grant Thornton

В ВНД КО должны быть установлены требования к КИР и к их документированию, включающие:

✓количественное измерение КИР;
✓способы расчета КИР, в том числе с использованием средств автоматизации;
✓периодичность (не реже одного раза в год) проведения оценки в целях пересмотра КИР для обеспечения поддержания КИР в актуальном состоянии;
✓регулярность и своевременность расчета КИР с указанием сроков (периода) расчета КИР (например, в постоянном режиме, один раз в неделю, по состоянию на момент закрытия операционного дня);
✓процедуры валидации значений и данных КИР для проверки корректности расчета;
✓состав информации, используемой для расчета КИР, и ее источников, включая способ получения информации;
✓пороговые значения КИР с обоснованием их установления; наименования и элементы классификации операционных рисков, которые отслеживают КИР;
✓подразделение КО, ответственное за предоставление данных для расчета КИР и (или) расчет КИР;
✓порядок реагирования на превышение пороговых значений КИР.

Важно: *Для КО, являющихся операторами платежной системы или операторами услуг платежной инфраструктуры, требования к КИР должны быть установлены с учетом требований к определению показателей бесперебойности функционирования платежной системы, установленных в приложении 1 к Положению Банка России № 607-П, которые должны рассматриваться в качестве КИР.*

ФБК
Grant Thornton

Пункт 4.4 Глава 4 Приложения 1 к Указанию БР от 15.04.2015 № 3624-У

Внешняя информация

Было

КО должна накапливать внешнюю информацию о значительных убытках, понесенных кредитными организациями вследствие реализации операционного риска, включающую данные о суммах убытков, об объеме операций кредитных организаций в регионе, в котором были понесены убытки, о причинах и обстоятельствах их возникновения.

Стало

КО, использующая в целях оценки достаточности капитала на покрытие операционного риска методы, применяемые в международной практике, должна накапливать информацию о потерях, понесенных кредитными организациями вследствие реализации операционного риска, внешних событиях операционного риска, имевших место в кредитных и финансовых организациях, сопоставимых с ней по составу и масштабу операций, включающую данные о суммах потерь, об объеме операций кредитных организаций в регионе, в котором были понесены потери, о причинах и обстоятельствах их возникновения.

Пункт 4.4 Глава 4 Приложения 1 к Указанию БР от 15.04.2015 № 3624-У

Меры по минимизации риска

Было

В целях ограничения операционного риска КО разрабатывает комплекс мер, направленных на снижение вероятности наступления событий или обстоятельств, приводящих к убыткам вследствие реализации операционного риска, и (или) на уменьшение (ограничение) размера таких убытков. К числу таких мер относятся:

- ✓ разработка процедур совершения операций (сделок), порядка разделения полномочий и подотчетности по проводимым операциям (сделкам), позволяющих исключить (ограничить) возможность возникновения операционного риска;
- ✓ контроль за соблюдением установленных процедур;
- ✓ развитие систем автоматизации банковских технологий и защиты информации;
- ✓ страхование

Стало

В целях ограничения операционного риска КО разрабатывает **систему мер, направленных на снижение уровня операционного риска**. К числу таких мер относятся:

- ✓ разработка процедур совершения операций (сделок), порядка разделения полномочий и подотчетности по проводимым операциям (сделкам), позволяющих исключить (ограничить) возможность возникновения операционного риска;
- ✓ контроль за соблюдением установленных процедур;
- ✓ развитие систем автоматизации банковских технологий и защиты информации;
- ✓ страхование,
- ✓ **комплекс мероприятий, установленных подпунктом 4.1.5 пункта 4.1 Положения Банка России N 716-П.**

Мероприятия, направленные на предотвращение и (или) снижение вероятности событий ОР

- реализация КО способов контроля, например, указанных в пунктах 10, 11, 15, 17, 18, 28 приложения 3 к Положению 716-П, на этапах процессов, в которых выявлены операционные риски;
- изменение процессов и распределение обязанностей для обеспечения исключения конфликта интересов;
- документирование результатов выполнения процедур контроля в процессах;
- обеспечение контроля совершения операций и сделок;
- исключение совершения неконтролируемых) операций и сделок;
- другие мероприятия, разрабатываемые КО в зависимости от вида и характеристик процесса.

Мероприятия, направленные на ограничение размера потерь от реализации событий ОР

- установление пороговых значений в отношении полномочий принятия решений и определения лимитов операционного риска, контроля за соблюдением полномочий;
- внедрение элементов автоматизации участков процессов, при выполнении которых выявлены операционные риски по причине ошибок работников;
- разработка планов по обеспечению непрерывности и (или) восстановления критически важных процессов и функционирования информационных систем, и объектов информационной инфраструктуры;
- определение способа и порядка возмещения потерь от реализации событий операционного риска, например, с использованием переноса риска на участников финансового рынка, страхования;
- юридическое обеспечение судебных процессов с участием КО;
- юридическое сопровождение процессов, договоров и документации КО.

КЛАССИФИКАТОР СОБЫТИЙ ОПЕРАЦИОННОГО РИСКА

ТРЕБОВАНИЯ РЕГУЛЯТОРА

Информация о событиях операционного риска должна быть классифицирована кредитной организацией в соответствии с главой 3 Положения Банка России N 716-П **в зависимости от состава и масштаба операций**

3624-У

Кредитная организация (головная кредитная организация банковской группы) для всех видов операционного риска определяет во внутренних документах **единый классификатор** событий операционного риска в разрезе элементов

716-П

Элементы событий ОР

- Источники
- Типы событий
- Направления деятельности
- Виды потерь

Источники событий ОР

У одного и того же события ОР может быть один источник или несколько источников. В случае если КО определено более одного источника ОР, в отношении реализовавшегося события в базе событий указываются все выявленные источники события ОР и определяет наиболее значимый источник ОР.

Недостатки процессов	Действия персонала и других связанных с кредитной организацией лиц	Сбои систем и оборудования	Внешние причины
Ненадежная и (или) неэффективная организация внутренних процессов управления КО и совершения банковских и других операций, а также несоответствие указанных процессов деятельности КО и (или) требованиям законодательства РФ	Недостатки, связанные с действиями персонала КО (непреднамеренные ошибки, умышленные действия или бездействие) и других связанных с кредитной организацией лиц, включая собственников, а также лиц, связанных с КО в рамках агентских отношений по выполнению работ (оказанию услуг) от лица КО	Отказы и (или) нарушения функционирования применяемых кредитной организацией информационных, технологических и других систем, оборудования и (или) несоответствие их функциональных возможностей и характеристик потребностям КО	Воздействие внешних причин, включая действия третьих лиц, в том числе действия суда и исполнительных органов государственной власти, Банка России, других организаций, а также другие воздействия внешнего характера

Типы событий ОР

Преднамеренные действия персонала

Совершение работниками КО и другими связанными с КО лицами, включая собственников, а также физическими лицами, связанными с КО в рамках агентских отношений по выполнению работ (оказанию услуг) от лица КО преднамеренных действий или преднамеренное бездействие указанных лиц, направленные на присвоение, хищение, уничтожение, нанесение ущерба материальным и нематериальным активам или другому имуществу КО и (или) средствам клиентов, нарушение процессов, препятствующие достижению целей КО организации, в том числе умышленное несоблюдение нормативных актов или ВНД КО в целях извлечения материальной и нематериальной выгоды

Преднамеренные действия третьих лиц

Совершение третьими лицами преднамеренных действий, направленных на присвоение, хищение, уничтожение, нанесение ущерба материальным и нематериальным активам или другому имуществу КО и (или) средствам клиентов (за исключением вандализма), нарушение процессов и ухудшение работы систем, препятствующих достижению стратегии развития КО или нарушающих законодательство РФ, в том числе приобретение прав на имущество КО обманным путем

Ущерб материальным активам

Ущерб материальным активам КО вследствие снижения стоимости имущества, потери свойств материальных активов КО в результате стихийных бедствий, техногенных катастроф, эпидемий, беспорядков, вандализма и военных действий

Нарушение кадровой политики и безопасности труда

Нарушение со стороны КО трудового законодательства, кадровой политики, условий труда и безопасности, требований по охране труда или охране здоровья, связанных с выплатами работникам КО по исковым требованиям (в том числе по искам о возмещении морального и материального вреда или искам в связи с дискриминацией), а также вследствие прекращения трудовых отношений

Нарушение и сбои систем и оборудования

Нарушение и сбои систем и оборудования, обеспечивающих функционирование деятельности КО

Нарушение прав клиентов и контрагентов

Нарушение со стороны КО прав клиентов и контрагентов, включая нанесение им ущерба, при оказании им услуг и совершении операций, включая нарушение условий договоров и сохранности конфиденциальной информации, ставшей доступной КО в процессе взаимодействия с клиентами и контрагентами по операциям и сделкам при оказании услуг, предоставлении банковских услуг с условием приобретения клиентом сопутствующих услуг КО или третьих лиц и нарушение законодательства в сфере защиты прав потребителей, а также антимонопольного законодательства

Нарушение организации, исполнения и управления процессами

Нарушение организации, исполнения и управления процессами КО, включая ошибки при обработке операций, недостатки обеспечения функционирования процессов, недостатки систем управления рисками, внутреннего контроля, учета и отчетности, системы обеспечения информационной безопасности, недостатки внутренних процедур ПОДФТ/ФРОМУ, недостатки в процессах взаимоотношений с торговыми контрагентами и поставщиками

Направления деятельности

- **Корпоративное финансирование** - оказание услуг юридическим лицам, органам государственной власти и местного самоуправления по организации доступа к рынкам капитала, оптимизации структуры активов и повышению качества корпоративного управления, слияниям и поглощениям, оказанию консультационных услуг финансового посредничества, в том числе при организации синдицированного кредитования;
- **Операции и сделки на финансовом рынке** - осуществление операций и сделок с финансовыми инструментами торгового портфеля;
- **Розничное банковское обслуживание** - оказание банковских услуг розничным клиентам, кроме брокерских и депозитарных услуг;
- **Коммерческое банковское обслуживание корпоративных клиентов** - оказание юридическим лицам банковских услуг, за исключением услуг корпоративного финансирования;
- **Осуществление переводов денежных средств, платежей и расчетов через платежные системы** - осуществление переводов денежных средств, платежей и расчетов через платежные системы, в том числе платежную систему Банка России, в которых КО выступает как оператор по переводу денежных средств, в том числе платежей по собственным операциям, за исключением внутрибанковских операций по организации услуг по проведению платежей, расчетов и взаимодействия с клиентом в рамках предоставления банковских услуг, относящихся к основным направлениям деятельности, указанных в предыдущих пунктах;
- **Управление активами** - правление активами клиентов по договорам доверительного управления;
- **Агентские и депозитарные услуги** – оказание агентских и депозитарных услуг, в том числе услуг по хранению сертификатов ценных бумаг и (или) их учету, обеспечению сохранности активов и документов клиентов;
- **Розничное брокерское обслуживание** - брокерское обслуживание розничных клиентов;
- **Обеспечивающие и организационные направления деятельности**, например,

✓ бухгалтерский учет,
✓ административно-хозяйственная деятельность,
✓ управление рисками,
✓ деятельность по обеспечению функционирования информационных систем,
✓ обеспечение физической безопасности, противопожарной безопасности и охраны труда,
✓ юридическое сопровождение,
✓ управление персоналом (обеспечение деятельности кредитной организации).

Уровень критичности процессов

Класс процесса	Характеристика
Критически важные	Процессы обеспечивают выполнение • операций КО, указанных в пунктах 1-4 и 9 части первой статьи 5 Федерального закона «О банках и банковской деятельности» • ведение бухгалтерского учета, представление отчетности в Банк России • поддержание ликвидности, • выполнение операций на финансовых рынках, • кассовых операций, работу онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций, • соблюдение требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» , • Трудового кодекса РФ, • Федерального закона «О банках и банковской деятельности», • а также другие процессы, которые определены КО и прерывание функционирования которых оказывает влияние на выполнение обязательств перед клиентами и контрагентами
Основные	Процессы обеспечивают выполнение операций, предусмотренных статьей 5 Федерального закона «О банках и банковской деятельности», не отнесенных КО к критически важным процессам, и других операций и услуг, объем которых формирует объем расходов (доходов) более 5 процентов от дохода за год для целей расчета капитала на покрытие операционного риска КО
Обеспечивающие	
Прочие	Процессы, не отнесенные КО к критически важным процессам или основным процессам.

Виды потерь

Прямые

отраженные в бухгалтерском учете

- Снижение (обесценение) стоимости активов
- Досрочное списание (выбытие, потеря, уничтожение) материальных и нематериальных, финансовых активов
- Денежные выплаты клиентам и контрагентам в целях компенсации им во внесудебном порядке убытков, понесенных ими по вине третьих лиц
- Денежные выплаты работникам кредитной организации в целях компенсации им во внесудебном порядке убытков, понесенных ими по вине КО
- Потери от ошибочных платежей
- Расходы (выплаты), связанные с решениями суда и (или) представительством КО в суде
- Штрафы, наложенные исполнительными органами государственной власти и (или) Банком России
- Расходы на устранение последствий реализации события ОР, направленные на восстановление деятельности или на снижение потерь от реализовавшегося события ОР
- Отрицательный финансовый результат от невыгодных для кредитной организации сделок

Непрямые

не отраженные в бухгалтерском учете

Косвенные

определяемые расчетным методом в денежном выражении

- приостановления или прекращения совершения операций, вызванных событиями ОР
- неполученные доходы, связанные с непроведением отдельных сделок и операций
- повышение стоимости заимствований
- снижение рыночной стоимости акций КО или инструментов капитала
- потери, связанные с восстановлением ликвидности из-за оттока денежных средств

Качественные

Определяются с использованием экспертного мнения

- недополученные доходы от возникновение источников других видов риска
- недополученные доходы от приостановку деятельности в результате события ОР
- отток клиентов
- недополученные доходы от неисполнение обязательств по сделке и (или) неоказание услуги
- недополученные доходы от ограничения, приводящие к выполнению невыгодных для КО действий, накладываемые со стороны суда, исполнительных органов государственной власти, Банка России
- недополученные доходы от снижение качества предоставления услуг, выполнения операций
- недополученные доходы от утечку, потерю или искажение защищаемой, в том числе коммерческой, информации
- постановления, акты исполнительных органов государственной власти, Банка России, не связанные с уплатой штрафов
- снижение лимитов на межбанковское кредитование

Потенциальные

- потери, не реализовавшиеся в виде прямых и косвенных потерь, которые могли бы возникнуть при реализации не выявленных источников операционного риска и (или) при неблагоприятном стечении обстоятельств

ФБК
Grant Thornton

БАЗА СОБЫТИЙ ОПЕРАЦИОННОГО РИСКА

ТРЕБОВАНИЯ РЕГУЛЯТОРА

В кредитной организации (головной кредитной организации банковской группы) создается и обновляется **на постоянной основе** аналитическая база данных о событиях операционного риска и потерях, понесенных вследствие его реализации (далее - база событий).

3624-У

База событий **ведется в разрезе** участников банковской группы, направлений деятельности (структурных подразделений), видов операций (сделок). элементов

3624-У

База Событий (БС)

Аналитическая база данных о событиях операционного риска и потерях, понесенных вследствие его реализации.

Пункт 4.3 приложения 1 к Указанию Банка России от 15.04.2015 № 3624-У «О требованиях к системе управления рисками и капиталом кредитной организации и банковской группы»

ФБК
Grant Thornton

Важные принципы ведения БС

- Ведется на постоянной основе.

- Данные о событиях ОР и потерях от реализации событий ОР охватывают

✓ всю деятельность КО

✓ все организационные, информационные и технологические системы

✓ все регионы присутствия КО.

- В БС подробно отражается информации о причинах и обстоятельствах реализованных событий ОР.

- В ВНД устанавливается порог регистрации: величина прямых и непрямых потерь от реализации события ОР, при котором событие ОР регистрируется в БС (но не более 20 тысяч рублей). Исключение - преднамеренные действия персонала и третьих лиц, прочие потенциальные потери.

- При указании связи события ОР с другими видами риска (кредитным, рыночным, риском ликвидности, стратегическим, риском потери деловой репутации и другими) необходимо уточнять, является ли другой вид риска источником или следствием события ОР.

Структура БС

- уникальный порядковый идентификационный номер события ОР;
- идентификатор группы событий;
- дата регистрации события и время регистрации события в случае программно-аппаратной фиксации событий;
- дата, когда событие произошло или впервые началось (дата реализации) и время, когда событие произошло или впервые началось, в случае программно-аппаратной фиксации событий риска ИБ и других событий ОР;
- дату (и время), когда КО стало известно о событии операционного риска (дата выявления);
- дату (и время для событий риска ИБ) окончания события риска (дата окончания события) ;
- статус события операционного риска;
- подразделение, в котором произошло событие;
- подразделение, выявившее событие;
- описание события;
- категорию источника ОР;
- значимые источники операционного риска,;
- тип события ОР;
- вид ОР);
- связь с другими видами риска при наличии такой связи;
- идентификатор связанного события ОР в случае, если такая связь установлена;
- дополнительную классификацию типа события ОР в зависимости от вида риска;
- направление деятельности;
- процесс;
- этап процесса;
- информационную систему;
- меры, направленные на уменьшение негативного влияния ОР.

Расчет потерь

Чистые (фактические) потери от реализации события операционного риска определяются как потери за вычетом суммы возмещения

ФБК
Grant Thornton

Валовые потери

- **КО ежемесячно на отчетную дату определяет величину валовых потерь** от реализации событий операционного риска со статусом «оценка потерь от реализации события операционного риска не завершена» начиная от даты регистрации события операционного риска в базе событий и от начала календарного года (в случае, если событие операционного риска реализовалось ранее текущего календарного года) нарастающим итогом.

- Также в расчет валовых потерь КО включаются потери от реализации событий операционного риска, статус которых был переведен в статус «оценка потерь от реализации события операционного риска завершена», в течение отчетного месяца.

В расчет величины валовых потерь включаются

1. сумма прямых потерь от реализации события операционного риска, определяемых в соответствии с пунктом 3.12 Положения №716-П, включая обесценение, списание активов, отраженных на счетах бухгалтерского учета;

2. корректировка стоимости прямых потерь, не отраженных в бухгалтерском учете в течение текущего календарного года, связанных с перерасчетом величины прямых потерь от реализации события ОР прошлого периода, в случае, если отражение в бухгалтерском учете потерь длится более одного календарного года (распределенные во времени потери). При этом в случае такой корректировки потери рассчитываются в корреспонденции со счетами расходов текущего года;

3. сумма прямых потерь по событиям ОР, которые вызывают искажение финансовой отчетности КО за определенный отчетный период (календарный год), но которые могут быть полностью скорректированы в дальнейшем (например, при завершении расчетов, создании исправительных бухгалтерских записей и переоценке справедливой стоимости финансовых инструментов, при определении временных потерь).

В расчет величины валовых потерь НЕ включаются

1. расходы КО по договорам на поддержание и регулярное обслуживание систем инженерно-технического обеспечения;

2. внутренние и внешние расходы КО, направленные на улучшение деятельности после завершения оценки потерь от реализации ОР (модернизация, совершенствование, мероприятия по предотвращению риска, улучшению качества процессов, оценке рисков и расширению функционала по управлению ОР); выплата страховых премий;

3. расходы, связанные с доначислением резервов на возможные потери по ссудам, ссудной и приравненной к ней задолженности, формируемых в соответствии с пунктом 1.1 Положения Банка России № 590-П, по событиям ОР, повлекшим реализацию кредитного риска по конкретным ссудам, ссудной и приравненной к ней задолженности, за исключением случаев, когда указанные расходы возникли в результате реализации события операционного риска, тип которого указан в подпункте 3.6.1 пункта 3.6 Положения №716-П.

Возмещение потерь

Каждое **возмещение потерь должно быть связано с регистрацией в бухгалтерском учете** компенсации потери от реализации события операционного риска, отражено на счетах бухгалтерского учета в виде бухгалтерской записи по счетам доходов (прибылей), обратной бухгалтерской записи, другой бухгалтерской записи с указанием номера бухгалтерской записи (идентификатора бухгалтерской записи), даты записи

Виды возмещений потерь:

- возмещения, полученные в судебном порядке;
- возмещения, полученные во внесудебном порядке по соглашению сторон;
- страховые выплаты от одной или нескольких страховых организаций;
- возмещения, полученные от третьих лиц;
- возмещения от работников КО;
- возмещения, полученные из других источников;
- восстановление резерва на возможные потери по ссудам, ссудной и приравненной к ней задолженности в соответствии с Положением Банка России № 590-П и Указанием Банка России № 1584-У;
- восстановление резерва по прочим потерям и обязательствам некредитного характера в соответствии с Положением Банка России № 611-П.

Ответственность за ведение БС

В ВНД КО должны быть установлены следующие перечни:

- перечень должностей работников, ответственных за ведение базы событий;
- перечень должностей работников, предоставляющих информацию для базы событий;
- перечень должностей работников, определяющих потери от реализации событий операционного риска, занесенные в базу событий;
- перечень должностей работников, ответственных за проверку полноты информации в базе событий и сверку счетов бухгалтерского учета с информацией, отраженной в БС.

Информация о событиях ОР в БС подлежит ежегодной независимой оценке, проводимой уполномоченным подразделением.

ОТЧЕТНОСТЬ ПО ОР

Кто готовит - Подразделение, ответственное за организацию управления операционным риском

Ежедневно – Руководителю СУР

- Информации о событиях ОР, зарегистрированных в базе событий за отчетную дату, предшествующую дате подготовке информации, или предоставление доступа к БС

Ежеквартально – Руководителю СУР и КИО

- Отчет об управлении операционным риском, содержащий информацию о событиях операционного риска и потерях КО, о результатах проведенных процедур управления ОР;
- Отчет о событиях риска информационной безопасности;
- Отчет о фактических значениях контрольных показателей уровня операционного риска.

Ежегодно – Руководителю СУР, КИО, СД (НС)

- Отчет об управлении операционным риском за год.

Коллегиальный исполнительный орган кредитной организации (головной кредитной организации банковской группы) **рассматривает отчеты** по операционным рискам **в срок не позднее двадцати рабочих дней со дня получения** их на рассмотрение и дает поручения по разработке мероприятий, направленных на повышение качества системы управления операционным риском и уменьшение негативного влияния операционного риска, с указанием ответственных за реализацию мероприятий подразделений и сроков выполнения.

Отчеты по операционным рискам **должны храниться не менее десяти лет** со дня рассмотрения коллегиальным исполнительным органом кредитной организации (головной кредитной организации банковской группы).

ВНУТРЕННИЕ НОРМАТИВНЫЕ ДОКУМЕНТЫ

Основные ВНД по управлению ОР

- Политика управления операционным риском
- Внутренние документы, описывающие процедуры управления операционным риском, а также процедуры оценки эффективности функционирования системы управления операционным риском.

Дополнительно устанавливаются в ВНД следующие требования

- Требования к информационной системе, обеспечивающей управление операционным риском и включающей автоматизацию ведения базы событий и процедур управления операционным риском.

Необходимо организовать информационный обмен информационной системы, обеспечивающей управление операционным риском, с другими информационными системами КО, позволяющими получать первичную информацию о сбоях систем и оборудования, об ошибках, отклонениях в процессах КО и о реализации событий операционного риска, в зависимости от осуществляемых операций и (или) действующих процессов.

- Требования к управлению модельным риском

Модельный риск

Риск ошибок процессов разработки, проверки, адаптации, приемки, применения методик количественных и качественных моделей оценки активов, рисков и иных показателей, используемых в принятии управленческих решений.

Риску подвержены КО, использующие модели количественной оценки рисков.

Пункт 4.2 Приложения 1 к Указанию Банка России от 15.04.2015 года № 3624-У «О требованиях к системе управления рисками и капиталом кредитной организации и банковской группы»

ФБК
Grant Thornton

Требования к управлению модельным риском

- выявление потенциальных ошибок в процессах разработки, проверки, адаптации, приемки, применения методик количественных и качественных моделей оценки активов (далее - модели оценки активов), включая оценку влияния этих ошибок на качество и прогнозную точность моделей оценки активов;
- выявление недостоверности и неполноты данных, использованных при разработке и проверке моделей оценки активов, включая в том числе оценку влияния этих ошибок на качество моделей оценки активов, например, приводящих к невозможности определения значения одного или нескольких входных параметров модели оценки активов или существенных факторов, использованных в модели оценки активов;
- контроль за разработкой моделей оценки активов, проверка правильности применения методик и технологий моделирования, в том числе правильности постановки задачи на разработку, принимаемых допущений, использования в моделях оценки активов всех существенных факторов, оценки прогнозной точности моделей оценки активов, контроль за соответствием моделей оценки активов условиям внешней среды и внешним и внутренним факторам их применения;
- выявление ошибок в процессах регистрации, учета и отчетности о результатах разработки и применения моделей оценки активов;
- контроль за полнотой документации о разработке моделей оценки активов и ее применением;
- контроль за своевременностью калибровки моделей оценки активов, связанной с изменением внешних и внутренних факторов их применения и поступлением новых данных, свидетельствующих о снижении качества моделей оценки активов и их прогнозной точности;
- валидация моделей оценки активов (подразделением КО и (или) внешними экспертами);
- контроль качества валидации моделей оценки активов, в том числе корректности применения валидационных тестов и критериев, включая контроль за правильностью интерпретации результатов валидации и реагирования на эти результаты;
- контроль за внедрением моделей оценки активов в промышленную эксплуатацию, в том числе за имплементацией программного кода в автоматизированные системы КО;
- выявление ошибок в интерпретации результатов моделей оценки активов для принятия управленческих решений и бизнес-решений в КО, в том числе связанных с использованием моделей оценки активов в предметных областях, для которых они не разрабатывались и не валидировались.

ВНУТРЕННИЕ И ВНЕШНИЕ ОЦЕНКИ

Внутренние и внешние оценки

Оценка	Периодичность	Кто проводит
Оценки эффективности системы управления операционным риском.	Ежегодно	Уполномоченное подразделением и (или) организация, осуществляющая внешний аудит. КО определяет во ВНД уполномоченное подразделение, а также правила привлечения для оценки эффективности функционирования системы управления операционным риском внешних экспертов.
Качественная оценка уровня операционного риска, проводимая в отношении выявленных операционных рисков в дополнение к количественной оценке и включающая профессиональную оценку	Ежегодный план проведения качественной оценки, разрабатываемой подразделением, ответственное за организацию управления ОР	Выделенные для данной процедуры работники подразделений КО и (или) внешние эксперты с учетом установленных КО во внутренних документах правил привлечения внешних экспертов.
Самооценка ОР	Ежегодный план проведения качественной оценки, разрабатываемой подразделением, ответственное за организацию управления ОР	По установленной в ВНД методике (в виде анкетирования выделенных для данной процедуры работников подразделений КО)
Валидация моделей оценки активов, используемых в управлении модельным риском	Ежегодно	Подразделение КО или внешний эксперт

Внутренние и внешние оценки

Оценка	Периодичность	Кто проводит
Оценка эффективности функционирования системы управления риском информационной безопасности в рамках	Ежегодно	Уполномоченным подразделением и (или) внешним экспертом (специализированной организацией или квалифицированным внешним экспертом) по решению совета директоров (наблюдательного совета) кредитной организации
Оценка соблюдения кредитной организацией требований Положения Банка России № 382-П, Положения Банка России № 683-П, Положения Банка России от 9 января 2019 года № 672-П (для кредитных организаций - участников платежной системы БР)	Не реже одного раза в два года.	Внешний эксперт – «Проверяющая организация»
Независимая оценка соответствия уровня защиты информации в отношении объектов информационной инфраструктуры КО в соответствии с требованиями пункта 9 Положения Банка России № 683-П (для кредитных организаций).	Не реже одного раза в два года.	Внешний эксперт – «Проверяющая организация»
Тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры в соответствии с подпунктом 3.2 пункта 3 Положения Банка России № 683-П	Ежегодно	Внешний эксперт – «Проверяющая организация»
Независимая оценки качества данных в информационных системах	Не реже одного раза в год	Определяется КО в «Политике информационных систем»

Управления риском информационных безопасности: новые требования и важные нюансы

Черненко Александр

Директор FBK | Cybersecurity

Управления риском информационных безопасности: новые требования и важные нюансы

Черненко Александр

Директор FBK | Cybersecurity

«Новая» история?

- Термины «операционный риск» и «риск информационной безопасности» появились в Стандарте Банка России по ИБ в 2004 году (СТО БР ИББС 1.0-2004).
- С каждой версией стандарта риск-ориентированный подход развивался. При оценке соответствия требованиям СТО БР ИББС использовались группы показателей М13 "Выбор/коррекция подхода к оценке рисков нарушения ИБ и проведению оценки рисков нарушения ИБ» и М14 "Разработка планов обработки рисков нарушения ИБ»
- В 2010 были введены в действие Рекомендации в области стандартизации Банка России: «Методика оценки рисков нарушения информационной безопасности» (РС БР ИББС-2.2-2009)
- В 2010-11 г. на волне ужесточения требований в области защиты ПДн Стандарт Банка России стал де-факто обязательным для КО

Что такое риск информационной безопасности

РС БР ИББС-2.2-2009 «Методика оценки рисков нарушения ИБ»:

3.11. **Риск:** мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

3.12. **Риск нарушения информационной безопасности; риск нарушения ИБ[1]:** риск, связанный с угрозой ИБ.

3.13. **Угроза информационной безопасности; угроза ИБ:** угроза нарушения свойств ИБ — доступности, целостности или конфиденциальности информационных активов организации БС РФ.

ГОСТ Р ИСО/МЭК 27005-2010 «Менеджмент риска ИБ»:

3.2 **риск информационной безопасности** (information security risk): Возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации.

Примечание - Он измеряется исходя из комбинации вероятности события и его последствия.

Риск информационной безопасности

Риск реализации угроз безопасности информации, которые обусловлены недостатками процессов обеспечения информационной безопасности, в том числе проведения технологических и других мероприятий, недостатками прикладного программного обеспечения автоматизированных систем и приложений, а также несоответствием указанных процессов деятельности кредитной организации

Абзац 2 пункт 1.4 Положения Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

Что включает в себя риск ИБ

- риск преднамеренных действий со стороны работников кредитной организации и (или) третьих лиц с использованием программных и (или) программно-аппаратных средств, направленных на объекты информационной инфраструктуры кредитной организации (головной кредитной организации банковской группы) в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности информации, подготавливаемой, обрабатываемой и хранимой такими объектами, а также в целях несанкционированного присвоения, хищения, изменения, удаления данных и иной информации (структуры данных, параметров и характеристик систем, программного кода) и нарушения режима доступа (далее - киберриск)

- другие виды риска информационной безопасности, связанных с обработкой (хранением, уничтожением) информации без использования объектов информационной инфраструктуры

Что такое кибер-риск

Кибер-риск	
Что это	• Преднамеренные действия
Кто совершает	• Работники • Третьи лица
На что направлены	• Объекты информационной инфраструктуры
Цель действий	• Нарушение / прекращение функционирования объекта • Создание угрозы безопасности информации • Присвоение, хищение, изменение, удаление данных

База событий оперриска

- Все события риска ИБ должны фиксироваться в общей базе оперриска
- Событие риска информационной безопасности – инцидент ИБ, вследствие которого возникли прямые или непрямые потери
- Событию риска ИБ дополнительно присваивается вид операционного риска – риск ИБ.

ФБК
Grant Thornton

Классификация событий риска ИБ

- События риска информационной безопасности классифицируются **по источникам** операционного риска:
  - Недостатки процессов
  - Действия персонала и других связанных с кредитной организацией лиц
  - Сбои систем и оборудования
  - Внешние причины

- Также классифицируются **по уязвимостям** информационных систем и их компонентов, как источникам последующих уровней классификации источников событий…
- Кредитная организация во внутренних документах **определяет последующие уровни классификации** источников событий операционного риска.

Классификация

РС БР ИББС-2.2-2009

Приложение 1
Рекомендуемый перечень классов, основных источников угроз ИБ и их описание

Источник угрозы ИБ	Описание
Класс 1. Источники угроз ИБ, связанные с неблагоприятными событиями природного, техногенного и социального характера	
Пожар	Неконтролируемый процесс горения, сопровождающийся уничтожением материальных ценностей и создающий опасность для жизни людей. Возможные причины: поджог, самовозгорание, природное явление
Природные катастрофы, чрезвычайные ситуации и стихийные бедствия	Природные явления разрушительного характера (наводнения, землетрясения, извержения вулканов, ураганы, смерчи, тайфуны, цунами и т.д.)
Техногенные катастрофы	Разрушительный процесс, развивающийся в результате нарушения нормального взаимодействия технологических объектов между собой или с компонентами окружающей природной среды, приводящий к гибели людей, разрушению и повреждению объектов экономики и компонентов окружающей природной среды
Нарушение внутриклиматических условий	Негативное изменение климатических условий в помещениях, где расположены технические средства и/или находится персонал: значительные изменения температуры и влажности, повышение содержания углекислого газа, пыли и т.п. Возможные последствия: сбои, отказы и аварии технических средств, снижение работоспособности и нанесение ущерба здоровью персонала, нарушение непрерывности выполнения процессов, снижение

Источник угрозы ИБ	Описание
Класс 3. Источники угроз ИБ, связанные с деятельностью поставщиков/провайдеров/партнеров	
Зависимость от партнеров/клиентов	Зависимость от партнеров заставляет организацию полагаться на их информационную безопасность, организация должна быть уверена, что партнер сможет обеспечить должный уровень безопасности либо учитывать данный источник угроз
Ошибки, допущенные при заключении контрактов	Неточности и неопределенности в договоре с провайдером внешних услуг, которые могут создавать проблемы в работе заказчика

Порядок ведения базы событий риска ИБ

- Кредитная организация самостоятельно определяет, вести отдельную базу событий риска ИБ, или использовать общую базу событий
- Если ведется отдельная база, необходимо соблюдать общие требования к классификации событий риска (источники, типы событий, направление деятельности, виды потерь и прочее) и требования к ведению базы событий

Ключевые обязанности КО

Кредитная организация:

- обеспечивает **выявление, регистрацию и учет всех событий риска** информационной безопасности **с определением всех элементов классификации** …
- **определяет суммы потерь в разрезе видов потерь** в соответствии с пунктом 3.11 Положения 716-П *(прямые или непрямые)* и пунктом 4 приложения 5 *(дополнительные (специфические) виды прямых и непрямых потерь: потери денежных средств, компенсации, штрафы; потери от простоя объектов ИИ, рабочее время, удорожание техобслуживания)* с распределением по датам отражения в бухгалтерском учете, с раздельным учетом поступивших возмещений.

Что должна содержать система внутренних документов

Кредитная организация в целях управления риском ИБ определяет во внутренних документах порядок функционирования системы ИБ и обеспечивает его выполнение, в том числе:

- Политику ИБ
- Выявление и идентификацию риска ИБ, а также его оценку
- Участие совета директоров (наблюдательного совета) и коллегиального исполнительного органа кредитной организации в решении вопросов управления риском ИБ
- Распределение функций и ответственности коллегиального исполнительного органа и работников кредитной организации
- Определение должностного лица, ответственного за функционирование системы обеспечения ИБ
- Защиту от угроз безопасности информации и операционную надежность

Что должна содержать система внутренних документов (продолжение)

- выявление событий риска ИБ, включая:
  - обнаружение компьютерных атак
  - рассмотрение обращений клиентов, контрагентов, работников и третьих лиц, связанных с нарушением ИБ
  - выявление и регистрацию инцидентов защиты информации
  - выявление уязвимостей и фактов компрометации объектов информационной инфраструктуры
- порядок реагирования на выявленные события риска ИБ и восстановления деятельности кредитной организации в случае реализации таких событий
- обмен информацией о событиях риска информационной безопасности, в том числе об инцидентах защиты информации, и предоставление данных в Банк России

Что должна содержать система внутренних документов (продолжение)

- организацию ресурсного (кадрового и финансового) обеспечения, включая установление требований к квалификации работников кредитной организации
- повышение осведомленности, обучение и развитие навыков работников в области противодействия угрозам безопасности информации
- установление и реализацию программ контроля, в том числе программ аудита
- соответствие фактических значений контрольных показателей уровня риска информационной безопасности принятым в кредитной организации значениям
- планирование, реализацию, контроль и совершенствование комплекса мероприятий, направленных на повышение эффективности управления риском ИБ и уменьшение негативного влияния риска ИБ

ФБК
Grant Thornton

Что должна содержать система внутренних документов (продолжение)

- выполнение требований к обеспечению защиты информации при осуществлении банковской деятельности, связанной с осуществлением перевода денежных средств (683-П, п.5)
- процессы применения прикладного программного обеспечения автоматизированных систем и приложений (683-П, п.4)
- ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры (683-П, п.3.2)
- независимую оценку соответствия уровня защиты информации в отношении объектов информационной инфраструктуры кредитной организации (683-П, п.9)

ФБК
Grant Thornton

Что должно быть зафиксировано в Политике ИБ

- функции и ответственность коллегиального исполнительного органа и работников кредитной организации в рамках управления риском ИБ
- основные принципы функционирования системы обеспечения информационной безопасности
- сигнальные и контрольные значения контрольных показателей уровня риска информационной безопасности
- основные принципы организации контроля за функционированием системы обеспечения информационной безопасности

Что должно быть зафиксировано в Политике ИБ

- требования к созданию ресурсных (кадровых и финансовых) условий системы обеспечения информационной безопасности
- требования к внешним контрагентам, выполняющим функции обеспечения информационной безопасности (аутсорсингу), а также определение порядка взаимодействия и распределения ответственности между ними

Политика ИБ утверждается коллегиальным исполнительным органом, который несет ответственность за соблюдение требований Политики

Функции службы ИБ (в целях обеспечения ИБ)

- Разработка Политики ИБ
- контроль осуществления работниками кредитной организации мероприятий в области обеспечения информационной безопасности и защиты информации
- осуществление планирования и контроля процессов обеспечения ИБ
- разработка предложений по совершенствованию процессов обеспечения ИБ
- составление отчетов по обеспечению ИБ и направление их должностному лицу, ответственному за обеспечение ИБ
- осуществление других функций, связанных с обеспечением ИБ, предусмотренных внутренними документами кредитной организации

Функции службы ИБ (в целях управления риском ИБ)

- соблюдение процедур управления операционным риском, в части идентификации, сбора и регистрации информации о событиях риска ИБ и потерях в базе событий, мониторинга риска ИБ
- ведение базы событий риска ИБ
- участие в реализации процессов в рамках комплекса мероприятий, направленных на повышение эффективности управления риском ИБ и уменьшение негативного влияния риска ИБ
- оценка эффективности управления риском ИБ
- составление отчетов по событиям риска ИБ и направление их в службу управления рисками и должностному лицу, ответственному за обеспечение ИБ

Функции службы ИБ (в целях управления риском ИБ)

- осуществление мониторинга сигнальных и контрольных значений контрольных показателей уровня риска ИБ (оценка эффективности функционирования системы управления операционным риском по «качественной» шкале)
- участие в разработке внутренних документов в области управления риском ИБ
- информирование работников кредитной организации по вопросам, связанным с управлением риском ИБ
- осуществление других функций, связанных с управлением риском ИБ, предусмотренных внутренними документами кредитной организации

Отчетность по рискам ИБ

- Служба информационной безопасности формирует специализированные отчеты по рискам ИБ, направляемые на рассмотрение коллегиальному исполнительному органу кредитной организации, в дополнение к отчетам, формируемым подразделением, ответственным за организацию управления операционным риском

- Отчеты по результатам аудитов по требованиям Положения Банка России № 382-П
- Сводные отчеты, направляемые должностному лицу, ответственному за обеспечение ИБ, и коллегиальному исполнительному органу кредитной организации
- Кредитная организация устанавливает во внутренних документах порядок и сроки предоставления данных отчетов

Независимая оценка эффективности системы управления операционным риском проводится не реже 1 раза в год

Общие рекомендации в части управления риском ИБ

Не пытайтесь «натянуть» систему управления оперрисками на информационную безопасность двигайтесь навстречу, адаптируя существующие процессы

Актуализируйте имеющиеся процессы управления рисками ИБ и инцидентами ИБ

Руководствуйтесь преимущественно «профильными» документами Банка России (382-П, 683-П и ГОСТ Р 57580.1, стандарты и рекомендации СТО/РС) или международными стандартами

Обзор Положения БР №716-П в части управления риском информационных систем

Карпушкин Алексей

Ведущий эксперт, руководитель направления по ИТ-аудиту
Департамент аудиторских и консультационных услуг финансовым институтам ФБК Grant Thornton

ФБК
Grant Thornton

Риск информационных систем

Риск отказов и (или) нарушения функционирования применяемых кредитной организацией информационных систем и (или) несоответствия их функциональных возможностей и характеристик потребностям кредитной организации

Абзац 3 пункт 1.4 Положения Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе

ФБК
Grant Thornton

ДОКУМЕНТИРОВАНИЕ ПОЛОЖЕНИЙ ПО УПРАВЛЕНИЮ РИСКОМ ИНФОРМАЦИОННЫХ СИСТЕМ КАК ОБЯЗАННОСТЬ КРЕДИТНОЙ ОРГАНИЗАЦИИ

Глава 8 Положения ЦБ №716-П

Требования к кредитным организациям в части рисков ИС:

- Определить во внутренних документах порядок управления риском информационных систем, включая мероприятия и процедуры по обеспечению требований к непрерывности и качеству функционирования информационных систем и обеспечению качества данных в информационных системах;

- Обеспечить проведение подразделениями кредитной организации мероприятий, направленных на:

  - ✓ повышение качества системы управления риском информационных систем;
  - ✓ снижение уровня риска информационных систем и сопряженных с ним рисков информационной безопасности, влияющих на информационные системы (в том числе рисков уничтожения (искажения, безвозвратного удаления) носителей и (или) хранилищ информации и данных, хранящихся в информационных системах).
  - ✓ выявление, оценку, разработку форм (способов) контроля;

Пример. Порядок управления риском информационных систем

Приложение 3

к Положению по управлению операционными рисками в [redacted]

Классификация источников операционного риска

Код	Тип источников операционного риска (1-й уровень)	Код	Источники операционного риска (2-й уровень)	Код	Источники операционного риска (3-й уровень)
ИР 1	Сбои оборудования	ИР 1.1	Сбои компьютерного оборудования	ИР 1.1.1	Сбои серверов
				ИР 1.1.2	Сбои в работе банкоматов
		ИР 1.2	Сбои в системе видеослежения	ИР 1.1.3	Сбои в работе персональных компьютеров на местах
		ИР 1.3	Сбои в сигнализационной системе		
		ИР 1.4	Сбои при передаче данных в электронном виде		
ИР 2	Сбои программного обеспечения и информационных технологий	ИР 2.1	Сбои в работе программного обеспечения	ИР 2.1.1	"Зависание"
				ИР 2.1.2	Программные ошибки (в расчетах)
				ИР 2.1.3	Несовместимость модулей
				ИР 2.1.4	Отказ в обслуживании
				ИР 2.1.5	Прочие сбои
		ИР 2.2	Недостатки в хранении, поддержке данных	ИР 2.2.1	Недостатки в архитектуре баз данных
				ИР 2.2.2	Отсутствие дополнительных аналитических признаков и регистров учета данных, снижающих качество бизнес-процессов
				ИР 2.2.3	Недостатки в обработке данных

Пример. Основные ИТ процессы, связанные с ними риски и контрол

ФБК
Grant Thornton

Примеры рисков и контролей категории Управления Изменениями

Риск	Контроль
УИ – Р01 Вносимые в систему изменения, в числе которых изменения логики, функционала, форм, интерфейса или отчетов, не соответствуют требованиям Бизнеса или ИТ.	УИ-К01 Перед разработкой запросы на изменения авторизуются руководителем бизнес-подразделения
УИ – Р02 Вносимые в систему изменения, в числе которых изменения логики, функционала, форм, интерфейса или отчетов, работают с отклонением от запрошенных требований в связи с отсутствием достаточного тестирования со стороны сотрудника, отличного от разработчика.	УИ-К02 Программное изменение (включая официальные изменения от вендора) тестируется в тестовой среде специалистами ИТ и/или представителями бизнес-подразделений.
УИ – Р03 Изменения системы, внесенные в рабочую среду, не согласованны	УИ-К03 После тестирования и перед переносом в продуктивную среду изменения утверждается руководителями бизнес-подразделения или/и ИТ.
УИ – Р04 Неавторизованные изменения переносятся в среду промышленной эксплуатации по причине наличия у разработчиков доступа на изменения в рабочую среду.	УИ-К04 Доступ к продуктивной среде и к средствам переноса изменений в продуктивную среду ограничен списком авторизованных сотрудников, которые не являются разработчиками.

Примеры рисков и контролей категории Управления Доступом

Риск	Контроль
УД-Р01 Получение несанкционированного доступа к ИТ-среде из-за отсутствия достаточного контроля за аутентификацией и настройками безопасности	УД-К01 Парольные настройки ИТ среды на уровне Приложения, домена и если применимо на уровне ОС и СУБД соответствуют требованиям безопасности и уровню ассоциированного риска
	УД-К03 Ключевые настройки безопасности (помимо парольных) ИТ среды на уровне Приложения, ОС, СУБД (если применимо) соответствуют требованиям безопасности и уровню ассоциированного риска
	УД-К04 Пароли, установленные по умолчанию, стандартных учётных записей на уровне Приложения, если применимо, на уровне ОС, СУБД, изменены или же соответствующие учетные записи заблокированы
	УД-К05 Встроенная учетная запись “Гость” на уровне домена заблокирована. Встроенная учетная запись “Администратор” на уровне домена заблокирована или переименована, пароль изменен
УД-Р02 Созданные учетные записи не были должным образом авторизированы. Нарушается принцип разграничения полномочий при управлении правами доступа к ИТ-среде.	УД-К06 Предоставление/изменение прав доступа к системе заблаговременно авторизуется соответствующим руководителем.
УД-Р04 Неавторизованное прямое изменение данных	УД-К11 Доступ к системным ресурсам и утилитам разрешен ограниченному кругу сотрудников ИТ в соответствии с их должностными полномочиями

Примеры рисков и контролей категории Управления Прочими ИТ процессами

Риск	Контроль
УП-Р01 Проблемы, связанные с оборудованием или программным обеспечением могут привести к потере или искажению финансовых данных	УП-К01 Проводится периодическое резервирование приложений и данных на резервных серверах/носителях, отличных от основных серверов
	УП-К02 Ведется журнал успешных/неуспешных задач по резервированию данных. Статус процедур резервирования отслеживается на постоянной основе ответственным специалистом и/или специалисты информируются о проблемах с выполнением процедур резервного копирования
УП-Р02 Задания по расписанию выполняются некорректно или не в полном объеме.	УП-К03 Список заданий, выполняемых автоматически, ограничен и контролируется при помощи журналирования и анализа произведенных действий (в том числе изменение финансовых данных).

РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННЫХ СИСТЕМ С УЧЕТОМ ТРЕБОВАНИЙ БАНКА РОССИИ

Политика информационных систем

Политика информационных систем - взаимосвязанная совокупность технических и программных средств, других объектов информационной инфраструктуры, содержащейся в базах данных информации и обеспечивающих ее обработку технологий в рамках реализации мероприятий поддержки и обеспечения непрерывности функционирования процессов кредитной организации.

Содержание Политики ИС:

1. функции и полномочия подразделений, ответственных за обеспечение функционирования ИС и их компонентов;
2. должностное лицо, ответственное за обеспечение функционирования ИС и координацию деятельности ответственного подразделения (из п.1);
3. реестр ИС;
4. требования к ИС;
5. порядок информационного взаимодействия в рамках реализации Политики;
6. отчетность подразделений и должностного лица (п.1-2) перед коллегиальным исполнительным органом кредитной организации.

Разделы 1-2 Политики информационных систем. Пример - Ответственные подразделение и должностное лицо

ПОЛОЖЕНИЕ
об Отделе сопровождения банковских систем
Управления информационных технологий
ЗАО [redacted]

ГЛАВА 2
ОСНОВНЫЕ ЗАДАЧИ И ФУНКЦИИ ОТДЕЛА

6. Основными задачами Отдела являются:

6.1. создание и эксплуатация информационной инфраструктуры Банка;

6.2. обеспечение качественного и бесперебойного функционирования информационной системы Банка;

6.3. внедрение и сопровождение информационных систем;

6.4. внедрение и развитие современных инновационных и информационных технологий, создание конкурентных преимуществ в информационной инфраструктуре Банка.

ГЛАВА 5
ОБЯЗАННОСТИ И ПРАВА НАЧАЛЬНИКА ОТДЕЛА

12. Начальник Отдела осуществляет руководство деятельностью Отдела в соответствии с настоящим Положением и заключенным с ним трудовым договором (контрактом) и **несет ответственность за полное, своевременное и качественное выполнение возложенных на Отдел задач и функций.**

Раздел 3 Политики информационных систем. Пример

Разделы 3 Политики информационных систем. Пример - Реестр ИС

Наименование информационной системы	Бизнес-процесс(ы), зависимый от информационной систем	Владелец бизнес-процесса (ФИО, должность, отдел)	Краткое описание архитектуры системы (самописная, коробочная, сложная и т.д.)	Разработчик системы (Банк, внешняя компания)
Центр межфилиальных расчетов (ЦМФР)	Межбанковские расчеты	Начальник ОРРМ УИТ Иванов И.И.	Коробочная	SoftClub
АБС Акцент		Директор УИТ Петров А.А.	Самописная	Банк
Процессинг платежных карточек Cortex	Карточки	Директор УБПК Абрамова А.А.	Коробочная	Cortex
Канцлер	СЭД	...	Коробочная	IBA
Colvir. Модуль "Расчетно-кассовые операции"		...	Коробочная	Colvir

Имя сервера(ов) БД и приложения (если применимо)				Операционная система на серверах	Имя базы данных			СУБД
Среда промышленной эксплуатации	Среда разработки	Среда тестировани	Резервное копирование		Среда промышленной эксплуатаци	Среда разработки	Среда тестирования	
CMFR101. БД:ora-vm-cmfr.	На стороне разработчика	cmft-test. БД:ora11-test-02.	CMFR102.		CMFR	На стороне разработчика	CMFRTS01	Oracle
accent. БД:ora-fc-02.	БД:ora11-test-03.	БД:ora11-test-03.	БД:ora-fc-14.	Linux Enterprise Server 11 (x86_64) VERSION = 11 PATCHLEVEL = 4	AWARD	OMAR	OMAR	Oracle
visa-lctx1, visa-lctx2 БД:dbcore	На стороне разработчика	d8t-tctx-colvir БД: d8t-lora-db	БД: d8-visa-lora-stb	HP-UX 11.31 SLES 15.1	CTX	На стороне разработчика	CTX	Oracle 18.3 SE
LDA01.			LDA02.	Windows Server 2012 R2				nsf
БД:ora-fc-20.	ora-fc-24.	ora-fc-26	БД:ora-fc-30.	SUSE Linux Enterprise Server 12 (x86_64) VERSION = 12 PATCHLEVEL = 7	CVB	CVBTS07	CVBTS03	Oracle

ФБК
Grant Thornton

Раздел 5 Политики информационных систем. Пример - Порядок информационного взаимодействия

Информационное взаимодействие

3. ОБЩЕЕ ОПИСАНИЕ ПОДДЕРЖКИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

3.1. Для получения поддержки Пользователь должен обратиться с Запросом в Service-Desk, выбирая необходимую услугу.

3.2. Сводный список услуг (Приложение 1) представляет собой перечень услуг предоставляемых сотрудникам Банка , а также и другим лицам в рамках выполнения своих функциональных обязанностей, решаемых через ServiceDesk.

3.3. Сводный список услуг является источником данных для настройки специализированного ПО Naumen Service Desk и построения системы службы поддержки пользователей.

3.4. Взаимодействие Пользователей со специалистами Банка по вопросам поддержки, минуя ServiceDesk, не допускается.

ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ К ИНФОРМАЦИОННЫМ СИСТЕМАМ С УЧЕТОМ ИХ ВЛИЯНИЯ НА ОБЕСПЕЧЕНИЕ БЕСПЕРЕБОЙНОЙ РАБОТЫ ПРОЦЕССОВ КРЕДИТНОЙ ОРГАНИЗАЦИИ

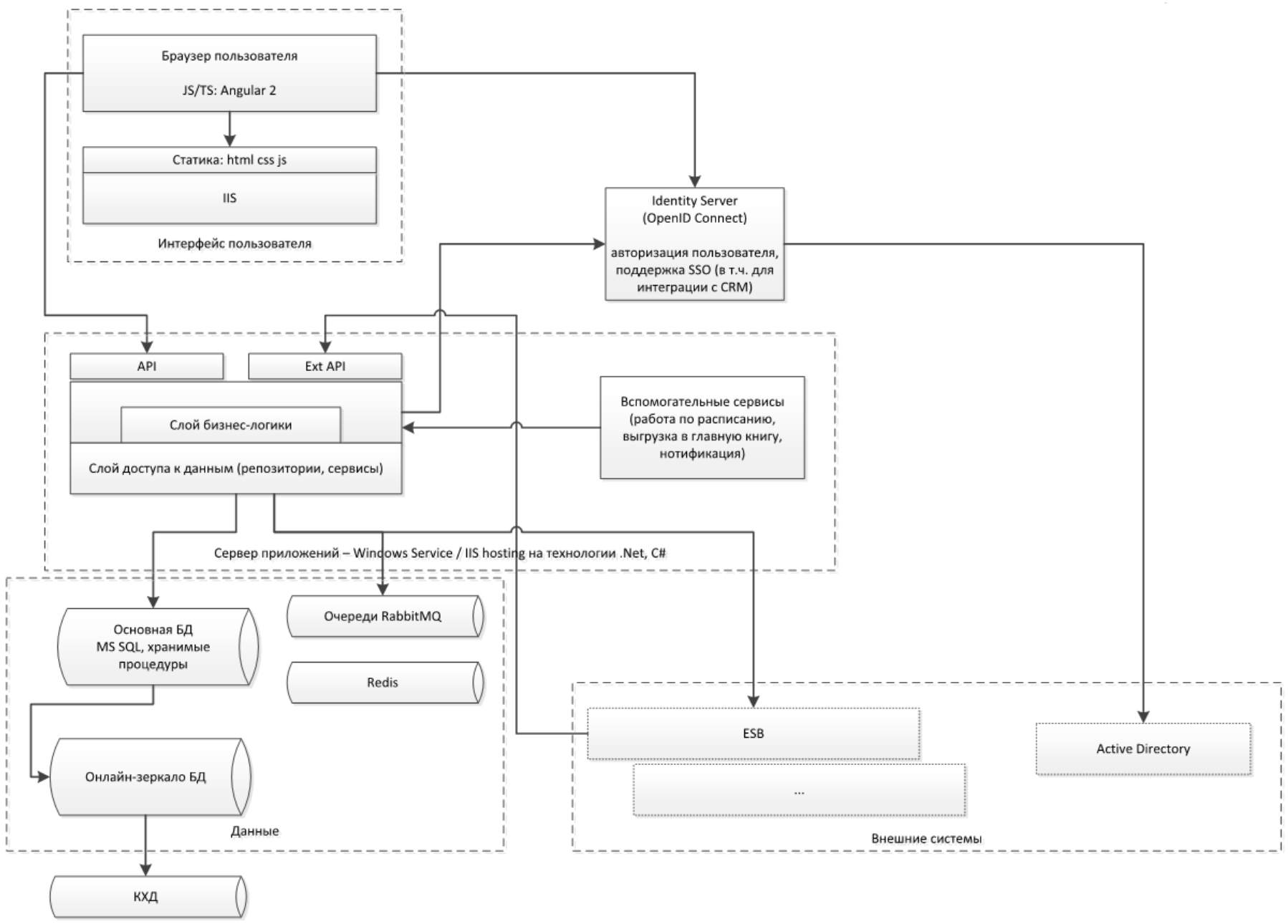
Требования к ИС с учетом их влияния на обеспечение бесперебойной работы процессов кредитной организации

1. Требования к структуре информационных систем;
2. Требования к стандартизации и унификации, используемые при создании, модернизации и эксплуатации ИС;
3. Требования к надежности функционирования ИС;
4. Требования к обеспечению качества данных в ИС;
5. Дополнительные требования к ИС и их функционированию с учетом осуществляемых операций и (или) действующих процессов, уровня и сочетания принимаемых рисков, текущих и стратегических планов развития и доступных возможностей.

- ✓ Методика обеспечения качества данных в информационных системах, обеспечивающих критически важные процессы

- ✓ Порядок обеспечения качества данных в информационных системах, обеспечивающих критически важные процессы

Блок 1. Требования к структуре информационных систем. Пример



ФБК
Grant Thornton

Блок 2. Требования к стандартизации и унификации, используемые при создании, модернизации и эксплуатации ИС. Пример

ПОЛОЖЕНИЕ
о процессе приобретения, разработки
и модификации банковского прикладного
программного обеспечения в ЗАО [redacted]

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение разработано в соответствии с Положением об управлении операционным риском в ЗАО [redacted] и регламентирует последовательность выполнения и содержание процедур при планировании и проведении мероприятий по разработке и модификации прикладного программного обеспечения (далее - БППО), используемого для автоматизации деятельности ЗАО [redacted] (далее – Банк), а также порядок взаимодействия Управления информационных технологий, Управления банковских платежных карточек и иных структурных подразделений Банка в процессе разработки и модификации БППО.

Блок 3. Требования к надежности функционирования ИС (Пример 1)

1-й приоритет – должно быть восстановлено в течение семи дней после объявления аварии

Функция	Критический срок	Критическое приложение	Жизненно важно (Да/Нет)
Программирование	7 дней	1С	Y
Бухгалтерский учет / Производство / Продажи	7 дней	1С	Y
Заработная плата	7 дней	1С	Y
Отгрузка	7 дней	1С	Y
Критические серверы	7 дней	E-mail 1С Directum	Y

2-й приоритет – должно быть восстановлено в течение двух недель

Функция	Критический срок	Критическое приложение	Жизненно важно (Да/Нет)
Программирование	2 недели	Delphi	N

3-й приоритет – должно быть восстановлено в течение трёх или более недель

Функция	Критический срок	Критическое приложение	Жизненно важно (Да/Нет)
Продажи и маркетинг	3 или более недель	Портал для дилеров Oracle BI	N
Программирование	3 или более недель	Хранилище конфигураций 1С	N

Блок 3. Требования к надежности функционирования ИС (Пример 2)

Название услуги	**Поддержка «ИКД»**		
Описание услуги	Сервис предназначен для предоставления пользователям технической поддержки ПО «ИКД». Поддержка работоспособности системы. Доступ к сервису предоставляется на рабочих местах сотрудников Банка.		
Ключевые характеристики услуги	Поддержание работоспособности ПО «ИКД».		
Типы инциденты	Исправление реквизитов клиентов в ПО ИКД,		
Типы запросы на обслуживание	Заведение новых клиентов.		
Группа пользователей	Руководство Банка, ЦБУ/РКЦ, УКО, ОКК	УРПСБ	Прочие
Время предоставления	00:00-23:59	08:00-21:30	08:00-21:30
Критичность	Высокая	Средняя	Низкая
Время поддержки	Рабочие дни (за искл. пятницы): 8:30-17:30 Пятница: 8:30-16:15 Предпраздничные дни: (-1 час)	Рабочие дни (за искл. пятницы): 8:30-17:30 Пятница: 8:30-16:15 Предпраздничные дни: (-1 час)	Рабочие дни (за искл. пятницы): 8:30-17:30 Пятница: 8:30-16:15 Предпраздничные дни: (-1 час)
Время выполнения обращения (запроса) со срочностью **«Низкая»**	13	13	26
Время выполнения обращения (запроса) со срочностью **«Средний»**	1	13	13
Время выполнения обращения (запроса) со срочностью **«Высокая»**	0.5	1	13
График технических работ (время возможной недоступности услуги)	Услуга может быть недоступна для работы во время проведения обновления данных с 08:00-09:00 и 14:00-14:30, а также система недоступна для работы во время проведения технологических работ с 22:00 до 08:00		

ОСНОВНЫЕ ПОЛОЖЕНИЯ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ И КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Требования по обеспечению непрерывности и качества функционирования информационных систем

1. Разработка, реализация и контроль выполнения требований к информационным системам, обеспечивающим функционирование системы информационной безопасности;
2. Обеспечение условий эксплуатации инженерно-технических средств;
3. Регулярное (не реже одного раза в день) резервное копирование данных критически важных процессов;
4. Использование программного обеспечения, принятого в эксплуатацию с соблюдением требований к эксплуатации ИС и технических условий эксплуатации, описанных в эксплуатационной документации;
5. Наличие положения и стратегии по обеспечению непрерывности и восстановления функционирования информационных систем;
6. Проведение регулярных (не реже одного раза в год) оценок состава компонентов, архитектуры, информационной инфраструктуры и характеристик информационных систем на предмет их достаточности и эффективности для обеспечения функционирования процессов кредитной организации;
7. Ежегодное тестирование уязвимостей информационных систем и (или) их компонентов и других источников риска информационных систем;
8. Дополнительные требования к обеспечению непрерывности и качества функционирования информационных систем с учетом осуществляемых операций и (или) действующих процессов, принимаемых рисков, текущих и стратегических планов развития и доступных возможностей.

Блок 3. Требования к резервному копированию данных. Пример

3.2 Процедуры резервирования приложений и данных

Процедуры резервного копирования данных контролируется следующим образом: Системный администратор (ведущий специалист ГрРИиС ОИТ) ежедневно проводит проверку истории резервного копирования.
В зависимости от отчетного периода, ленты маркируются и направляются на хранение с установленной периодичностью их обмена.

3.2.1 Резервное копирование приложений/данных

Функционал	Периодичность копирования	ПО
Бухучет/ Производство/ Продажи	Ежедневно/Еженедельно	1С
Заработная плата	Ежедневно/Еженедельно	1С
Отгрузки	Ежедневно/Еженедельно	1С
СКД	Ежедневно/Еженедельно	1С
Утилиты	Ежедневно/Еженедельно	DBU
Документооборот	Ежедневно/Еженедельно	Директум
Программирование	Ежедневно/Еженедельно	1С (хранилище конфигураций)
Программирование	Ежедневно/Еженедельно	Средства разработки на sp02

Блок 5. Положения и стратегии по обеспечению непрерывности и восстановления функционирования ИС (Пример 1)

План обеспечения непрерывности и восстановления функционирования информационных систем

2018 год

1. Общие положения

1.1. Настоящий документ (далее – План ОНиВД АС БАНКА, или План) определяет комплекс мероприятий по предотвращению или своевременной ликвидации последствий возможного нарушения режима повседневного функционирования автоматизированной системы ПАО АКБ [redacted] (далее – АС БАНКА), вызванного нестандартными (далее – НС) и чрезвычайными ситуациями (далее – ЧС), а также способы и средства восстановления информации и процессов ее обработки в случае нарушения работоспособности АС БАНКА и ее основных компонентов.

1.2. В настоящем документе используются термины, сокращения и понятия, используемые в Плане ОНиВД.

2. Область применения документа

2.1. План ОНиВД АС БАНКА вводится в действие в случае, если принято решение об активации Плана ОНиВД, и при этом НС или ЧС повлияла на функционирование или доступность АС БАНКА.

2.2. Если не указано иное, то действия в рамках Плана ОНиВД АС БАНКА выполняются сотрудниками Департамента информационных технологий (далее – ДИТ).

Блок 5. Положения и стратегии по обеспечению непрерывности и восстановления функционирования ИС (Пример 2)

План восстановления после сбоев/катастроф (DRP - Disaster Recovery Plan)

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Описание Плана аварийного восстановления инфраструктуры ИТ

План аварийного восстановления инфраструктуры ИТ (далее – План аварийного восстановления ИТ, План) определяется как непрерывный процесс планирования, разработки, проверки и реализации процедур и процессов аварийного восстановления. Процесс предназначен для обеспечения эффективного и действенного возобновления жизненно важных бизнес-функций в случае крупного останова вычислительных телекоммуникационных операций АО [redacted].

С ростом зависимости предприятия от информационных технологий, которые поддерживают основные бизнес-процессы, рост и изменения бизнеса, для разработки Плана аварийного восстановления ИТ используется следующая методология:

- Идентификация критически важных приложений ИТ
- Процедуры резервного копирования
- Процедуры восстановления
- Внедрение (процедуры) «Начните отсюда в потенциальной чрезвычайной ситуации »
- План тестирования
- План технического обслуживания
- План переезда

Блок 7. Тестирование уязвимостей информационных систем и (или) их компонентов и других источников риска информационных систем. Пример

1. Результаты анализа защищенности

В результате анализа защищенности **со стороны внешнего нарушителя**, специалисты Исполнителя выявили возможность реализации следующих атак на ресурсы Системы Заказчика:

- Возможность перебора учетных данных к админ-панелям
- Возможность проведения Reflected-XSS атаки на основном домене [redacted]
- Возможность загрузки произвольных файлов в любую директорию на некоторых доменах
- Возможность получения исходных кодов приложений версий 2017 года из git репозиториев
- Возможность определить установленные модули и плагины и их версии
- Возможность формирования списка учетных данных сотрудников из метаданных документов, размещенных на корпоративном сайте Компании

2. Цель и задачи проведения работ

Целью данных работ являлось определение текущего уровня защищенности зоны [redacted] Заказчика по отношению к угрозам, связанным с возможными атаками злоумышленников изнутри локальной сети Заказчика.

Предполагалось, что основной целью злоумышленника является получение максимальных привилегий в локальной сети – прав администратора домена, либо получение административного доступ к отдельным серверам.

Задачи, решаемые в ходе проведения работ:

1. Поиск и попытка получения несанкционированного доступа к внутренним ресурсам зоны [redacted] Заказчика путем эксплуатации известных уязвимостей в сетевых сервисах и приложениях изнутри локальной сети Заказчика.

2. Формирование рекомендаций по повышению текущего уровня защищенности зоны [redacted] Заказчика на основе полученной информации о возможных путях получения несанкционированного доступа.

ОБЯЗАННОСТИ И ОТЧЕТНОСТЬ ЛИЦ, ОТВЕТСТВЕННЫХ ЗА РИСКИ ИНФОРМАЦИОННЫХ СИСТЕМ

Проверки и отчетность по рискам информационных систем (1)

Должностное лицо

самооценка рисков информационных систем в разрезе процессов с учетом требований главы 8

Отчет, не реже 1 раза в год

Службе управления операционным риском, и (или) др. органу

анализ необходимости пересмотра требований политики информационных систем

другие отчеты ДЛ и ОП в соответствии с порядком и периодичностью, установленными Политикой информационных систем

Ответственное подразделение

Отчет, не реже 1 раза в год

анализ необходимости пересмотра требований к информационным системам

Коллегиальный исполнительный орган

ФБК
Grant Thornton

Проверки и отчетность по рискам информационных систем (2)

Уполномоченное подразделение

оценка соблюдения кредитной организацией требований Главы 8 Положения №716-П

Отчет

не реже 1 раза в год

- **Совету директоров;**
- **КИО;**
- **ОП;**
- **Службе управления рисками.**

Отчеты о качестве данных, о проведении мероприятий контроля качества данных с периодичностью, определенной в Порядке обеспечения качества данных.

ФБК
Grant Thornton

Контакты спикеров для получения консультаций по интересующим вас вопросам

Майя Савицкая

Менеджер
Департамент аудиторских и консультационных услуг финансовым институтам
ФБК Grant Thornton
Mayya.Savitskaya@fbk.ru
+7 (495) 737 5353, доб. 3008, +7 (916) 327 2469

Александр Черненко

Директор FBK | Cybersecurity
bank@fbk.ru

Алексей Карпушкин

Ведущий эксперт, руководитель направления по ИТ-аудиту
Департамент аудиторских и консультационных услуг финансовым институтам
ФБК Grant Thornton
bank@fbk.ru

ФБК
Grant Thornton

Благодарим за внимание!

ул. Мясницкая, 44/1,
Москва, Россия 101990

Т: (495) 737 5353
Ф: (495) 737 5347
E: fbk@fbk.ru

fbk.ru

fbk-pravo.ru