ГОСТ Р 57580.3-2022 «УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ»

ТРЕБОВАНИЯ И ПОДХОДЫ К ОЦЕНКЕ ВЫПОЛНЕНИЯ

Антон Свинцицкий
Директор по консалтингу
АО «ДиалогНаука»

20 мая 2025 года, Москва

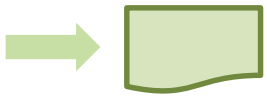
ДиалогНаука

Развитие управлением рисками ИБ

Добровольное присоединение

СТО БР ИББС 1.0-2004

СТО БР ИББС 1.0-2006
СТО БР ИББС 1.1-2007
СТО БР ИББС 1.2-2007



РС БР ИББС 2.2-2009
Методика оценки рисков

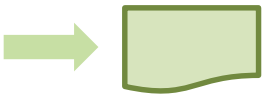
СТО БР ИББС 1.0-2014
СТО БР ИББС 1.1-2014
СТО БР ИББС 1.4-2018
Управление риском нарушения информационной безопасности при аутсорсинге
СТО БР БФБО-1.5-2018 (2023)
Управление инцидентами, связанными с реализацией информационных угроз, и инцидентами операционной надежности

Развитие управлением рисками ИБ

Добровольное присоединение

СТО БР ИББС 1.0-2004

СТО БР ИББС 1.0-2006
СТО БР ИББС 1.1-2007
СТО БР ИББС 1.2-2007



РС БР ИББС 2.2-2009
Методика оценки рисков

СТО БР ИББС 1.0-2014
СТО БР ИББС 1.1-2014
СТО БР ИББС 1.4-2018
Управление риском нарушения информационной безопасности при аутсорсинге
СТО БР БФБО-1.5-2018 (2023)
Управление инцидентами, связанными с реализацией информационных угроз, и инцидентами операционной надежности

Общеобязательные НПА

Положение БР 382-П (2012 г.)

Положение БР 851-П
Положение БР 757-П
Положение БР 802-П
Положение БР 821-П

ГОСТ Р 57580.1

Положение БР 716-П

ГОСТ Р 57580.3

Виды рисков ГОСТ Р 57580.3 и 716-П

Положение БР 716-П выделяет следующие виды операционного риска:

- ✓ риск реализации угроз безопасности информации (**риск информационной безопасности**);
- ✓ **операционная надежность, риск нарушения непрерывности деятельности**;
- ✓ **риск информационных систем**;
- ✓ другие.

ГОСТ Р 57580.3 оперирует понятиями:

- ✓ риск реализации угроз безопасности информации;
- ✓ операционная надежность, риск нарушения непрерывности деятельности

Виды рисков ГОСТ Р 57580.3 и 716-П

Риски ИБ:

Киберриски:

- ✓ Преднамеренные действия
- ✓ Работников/третьих лиц
- ✓ С использованием программных и (или) программно-аппаратных средств
- ✓ Направленны на объекты информатизации финансовой организации

Цели:

- ✓ Нарушения/прекращения функционирования объекты информатизации финансовой организации
- ✓ Создание угроз безопасности информации, несанкционированное присвоение, хищение, изменение, удаление данных и информации
- ✓ Нарушение режима доступа

Другие виды риска:

- ✓ Связанные с обработкой (хранением, уничтожением) информации без использования объектов информатизации
- ✓ Побуждение клиентов финансовой организации к осуществлению финансовых (банковских) операций

Цели:

- ✓ Мошенничество
- ✓ Кража с банковского счета клиентов финансовой организации

ГОСТ Р 57580.3-2022 и 716-П

Глава 7. Управление риском информационной безопасности Положения БР 716-П.

Требования к:

- ✓ документированию порядка управления риском ИБ
- ✓ документированию и выполнению порядка функционирования системы информационной безопасности
- ✓ фиксации инцидентов в базе событий риска ИБ и их классификации;
- ✓ политике ИБ;
- ✓ функциям подразделения, ответственного за обеспечение ИБ

ГОСТ Р 57580.3:

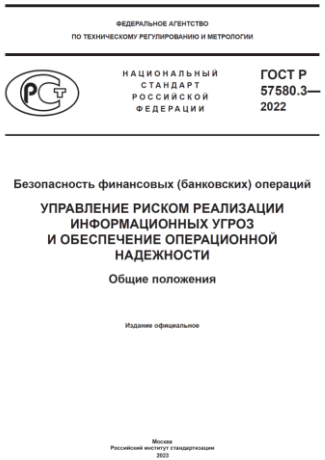
- ✓ Включает в свой состав
- ✓ Детализирует
- ✓ Расширяет
- ✓ Систематизирует

В том числе, посредством включения в область оценки требований:

ГОСТ Р 57580.1

ГОСТ Р 57580.4

ГОСТ Р 57580.3-2022


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.3— 2022

Безопасность финансовых (банковских) операций

УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Общие положения

Издание официальное

Москва
Российский институт стандартизации
2023

Устанавливает требования к системе управления **риском реализации информационных угроз**

↓

Направлено на обеспечение операционной надежности

↓

Связано с бизнес-процессами (технологическими процессами) и объектами информатизации

↓

Реализуется в «классической» модели PDCA

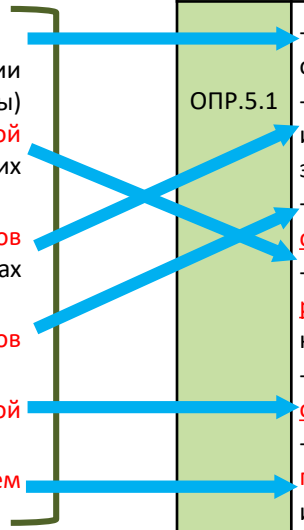
↓

Интегрировано в общую систему управления операционным риском

Пример 1

П. 7.9.1. Положения БР 716-П. *(выполнение подразделением, ответственным за обеспечение ИБ, функций в целях обеспечения ИБ)*:

- разработка политики информационной безопасности;
- контроль осуществления работниками кредитной организации (головной кредитной организации банковской группы) мероприятий в области обеспечения информационной безопасности и защиты информации и выполнения других задач…;
- осуществление планирования и контроля процессов обеспечения информационной безопасности в рамках комплекса мероприятий…;
- разработка предложений по совершенствованию процессов обеспечения информационной безопасности…;
- составление отчетов по обеспечению информационной безопасности …;
- осуществление других функций, связанных с управлением риском информационной безопасности…



Меры	Содержание мер системы управления риском реализации информационных угроз
ОПР.5	Установление функций и полномочий службы ИБ:
ОПР.5.1	- разработка и (или) пересмотр внутренних документов в области обеспечения операционной надежности и защиты информации; - планирование, реализация (в том числе установление требований) и контроль процессов обеспечения операционной надежности и защиты информации; - разработка предложений по совершенствованию процессов обеспечения операционной надежности и защиты информации…; - выявление и фиксация инцидентов, в том числе обнаружение реализации компьютерных атак и выявление фактов (индикаторов) компрометации объектов информатизации; - формирование отчетности по вопросам обеспечения операционной надежности и защиты информации…; - осуществление других функций, связанных с реализаций процессов обеспечения операционной надежности и защиты информации…

ГОСТ Р 57580.3 и 716-П

Пример 2

П. 7.7. Положения БР 716-П. *(Кредитная организация … определяет во внутренних документах порядок функционирования системы информационной безопасности и обеспечивает его выполнение, в том числе)*:

- ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры в соответствии с подпунктом 3.2 пункта 3 Положения Банка России N 683-П;

…

ГОСТ Р 57580.3

ВИО.13	Организация и выполнение деятельности по выявлению возможных уязвимостей критичной архитектуры путем выполнения мер, приведенных в таблице 4 ГОСТ Р 57580.4-2022

Меры УИ.22 - УИ.37 ГОСТ Р 57580.4

ГОСТ Р 57580.4

УИ.28	Регулярное тестирование на проникновение (симуляция компьютерных атак), в том числе тестирование на проникновение: - объектов информатизации, непосредственно взаимодействующих с сетью Интернет; - "внутренних" объектов информатизации, в том числе вычислительных сетей, на "границах" контуров безопасности
УИ.29	Применение риск-ориентированного подхода к выбору объектов информатизации, подвергаемых тестированию на проникновение, в том числе в части периодичности проведения тестирования на проникновение
УИ.30	Проведение сканирования на уязвимости и (или) тестирование на проникновение при существенных изменениях в критичной архитектуре и (или) внедрении новых объектов информатизации (автоматизированных систем)

Подходы к оценке выполнения 57580.3

Структура 57580.3 отличается от 57580.1 и 57580.4

ГОСТ Р 57580.1

ГОСТ Р 57580.4

Процессы

Требования к системе защиты/обеспечения операционной надежности

Направления

Требования к организации и управлению (ПЗИ, РЗИ, КЗИ, СЗИ/ПОН, РОН, КОН, СОН)

Шкала по 57580.2 для 57580.1

0 - выбрана;

1 - не выбрана

0 - полностью не реализуется;

0,5 - реализуется не в полном объеме;

1 - реализуется в полном объеме

ГОСТ Р 57580.3

Направления

- Планирование…
- Реализация…
- Контроль…
- Совершенствование…

состоящие из процессов

В условиях отсутствия утвержденной Методики оценки на текущем этапе организации могут самостоятельно определить способ оценки реализации мер

Подходы к оценке выполнения 57580.3

На текущем этапе качественные уровни соответствия 57580.3 НПА Банка России не заложены.

Отсутствует необходимость в общей (итоговой) оценке выполнения 57580.3 и разработки методики ее оценки.

Используемый ДиалогНаукой подход к оценке выполнения 57580.3 предусматривает количественную оценку мер стандарта по наиболее гибкой шкале, имеющей аналог для оценки направлений в 57580.2, а также ее качественную интерпретацию:

Оценка

0

0,5

1

Более гибко подходит к оценке совокупности мер из 57580.1 и 57580.4

Более гибко подходит к оценке мер 57580.3, состоящих из множества буллитов

Оценка «1» может быть присвоена только в случае реализации в полном объеме каждой из мер, входящих в оценку (например, как ВИО.13)

Подходы к оценке выполнения 57580.3

Оценка многосоставных мер предполагает расчет, включающий оценки всех подмер:

Мера	Содержание меры	Оценка меры	Подмера	Содержание подмеры	Оценка подмеры
ОПР.11	Установление политикой управления риском реализации информационных угроз в целях контроля за достижением целей управления таким риском состава КПУР, а также их сигнальных и контрольных значений по следующим группам:	0,67	ОПР.11.1	- группа КПУР, характеризующих уровень совокупных потерь финансовой организации в результате событий риска реализации информационных угроз	1
			ОПР.11.2	- группа КПУР, характеризующих уровень операционной надежности бизнес- и технологических процессов финансовой организации	1
			ОПР.11.3	- группа КПУР, характеризующих уровень несанкционированных операций (потерь клиентов финансовой организации) в результате инцидентов	0

Для оценки процессов управления риском реализации информационных угроз и обеспечение операционной надежности 57580.3 используется агрегированная оценка мер.

Оценка процессов направлений управления риском реализации информационных угроз и обеспечение операционной надежности агрегируется в оценку направлений 57580.3.

Подходы к оценке выполнения 57580.3

На период отсутствия утвержденной Банком России методики оценки выполнения 57580.3 количественные оценки интерпретируются следующим образом:

Оценка направления	Уровень соответствия
$E_i = 0$	Нулевой
$0 < E_i \leq 0{,}5$	Первый
$0{,}5 < E_i \leq 0{,}7$	Второй
$0{,}7 < E_i \leq 0{,}85$	Третий
$0{,}85 < E_i \leq 0{,}9$	Четвертый
$0{,}9 < E_i \leq 1$	Пятый

E_i - оценка соответствия i -го направления управления риском ИБ и обеспечения ОН;

i - номер направления управления риском ИБ и обеспечения ОН.

Подходы к оценке выполнения 57580.3

Направление «планирование» предусматривает не только документирование в ВНД требований, полномочий и т.п., но и затрагивает аспекты реализации.

Ряд требований содержит формулировки «Организация **и выполнение**».

Пример 1

Меры	Содержание мер системы управления риском реализации информационных угроз
ВИО.1	Организация и **выполнение** деятельности по анализу базы событий риска реализации информационных угроз

Отражение во внутренних документах соответствующей деятельности и распределение ролей по ее выполнению

Меры	Содержание мер системы управления риском реализации информационных угроз
ВИО.13	Организация и выполнение деятельности по выявлению возможных уязвимостей критичной архитектуры путем выполнения мер, приведенных в таблице 4 ГОСТ Р 57580.4-2022

Направление планирования 57580.4

Меры УИ.22 - УИ.37 ГОСТ Р 57580.4

Подходы к оценке выполнения 57580.3

Схожий подход к мерам (их реализации и оценке) наследуется в 57580.3 и далее, например, в направлении «Реализация системы управления риском реализации информационных угроз».

Ряд требований содержит формулировки «**Организация** и выполнение».

Пример 2

Меры	Содержание мер системы управления риском реализации информационных угроз
ВСР.3	**Организация** и выполнение деятельности по ведению базы событий риска реализации информационных угроз, включая:
ВСР.3.1	- определение порядка ведения базы событий
ВСР.3.2	- определение порядка установления величины потерь от реализации события риска реализации информационных угроз, при которой осуществляется регистрация таких событий в базе событий (порог регистрации), в том числе в соответствии с требованиями нормативных актов Банка России
ВСР.3.3	- определение перечня ролей и ответственных по ведению базы событий
ВСР.3.4	- определение порядка контроля за своевременностью отражения потерь от реализации событий риска реализации информационных угроз

Большинство мер стандарта, носят организационный способ реализации.

В совокупности меры приводят к необходимости отражения (и проверке) в документах значительного объема положений.

Учет мер 57580.1 и 57580.4 в ГОСТ Р 57580.3

ГОСТ Р 57580.3 является **базовым** в комплексе национальных стандартов "Безопасность финансовых (банковских) операций"

Помимо мер, перечисленных в таблицах ГОСТ Р 57580.3, в оцениваемые направления и процессы включаются меры, предусмотренные 57580.1 и 57580.4.

Включение в состав ГОСТ Р 57580.3 мер, связанных с планированием, реализацией, контролем и совершенствованием процессов, определенных 57580.1 и 57580.4

Включаемые меры 57580.1 и 57580.4

В состав направлений по управлению риском входят (включаются):

1

Направление: Планирование системы управления риском реализации информационных угроз

Процесс: Выявление и идентификация риска реализации информационных угроз, а также его оценка

Меры обеспечивающие: Идентификацию критичной архитектуры (таблица 1 ГОСТ Р 57580.4-2022)

2

Направление: Реализация системы управления риском реализации информационных угроз

Процесс: Планирование, реализация, контроль и совершенствование мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз

Подпроцесс: Защита от информационных угроз

Меры обеспечивающие: - Управление риском внутреннего нарушителя (таблица 14 ГОСТ Р 57580.4-2022);

- Предотвращение утечек информации (таблицы 1 - 12, 29 - 31 ГОСТ Р 57580.1-2017)

Включаемые меры 57580.1 и 57580.4

3

Подпроцесс: Реагирование на инциденты, связанные с реализацией информационных угроз, и восстановление после их реализации

Меры обеспечивающие: - Восстановление функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов (таблица 7 ГОСТ Р 57580.4-2022);

- Проведение анализа причин и последствий реализации инцидентов (таблица 8 ГОСТ Р 57580.4-2022);

- Организацию взаимодействия между подразделениями финансовой организации, а также между финансовой организацией и Банком России, причастными сторонами в рамках реагирования на инциденты и восстановления функционирования бизнес- и технологических процессов и объектов информатизации после их реализации (таблица 9 ГОСТ Р 57580.4-2022)

4

Подпроцесс: Выявление событий риска реализации информационных угроз

Меры обеспечивающие: - ыявление и фиксацию инцидентов, в том числе обнаружение компьютерных атак и выявление фактов (индикаторов) компрометации объектов информатизации (см. таблицу 5 ГОСТ Р 57580.4-2022)

Включаемые меры 57580.1 и 57580.4

5

Подпроцесс: Обеспечение осведомленности об актуальных информационных угрозах

Меры обеспечивающие: - организацию взаимодействия финансовой организации и причастных сторон, в том числе клиентов финансовой организации, при обмене информацией об актуальных сценариях реализации информационных угроз (таблица 15 ГОСТ Р 57580.4-2022);

- использование информации об актуальных сценариях реализации информационных угроз для цели обеспечения операционной надежности финансовой организации (таблица 16 ГОСТ Р 57580.4-2022);

- повышение осведомленности работников финансовой организации в части противостояния реализации информационных угроз (таблица 17 ГОСТ Р 57580.4-2022).

6

Направление: Контроль системы управления риском реализации информационных угроз

Процесс: Установление и реализация программ контроля и аудита

Меры обеспечивающие: - проведение сценарного анализа (в части возможной реализации информационных угроз) и тестирования с использованием его результатов готовности финансовой организации противостоять реализации информационных угроз в отношении критичной архитектуры (киберучения) (таблица 12 ГОСТ Р 57580.4-2022).

Меры, связанные с 57580.1 и 57580.4

Меры ГОСТ Р 57580.1 и 57580.4 учитываются при оценке 57580.3.

Пример 1

Меры	Содержание мер системы управления риском реализации информационных угроз
РМ.8	Планирование процессов применения организационных и технических мер, направленных на реализацию требований к процессам систем управления, определенных в рамках семейств стандартов ОН и ЗИ комплекса стандартов, включая:
РМ.8.1	- **планирование** применения организационных и технических **мер**, направленных на реализацию требований **к процессам системы защиты информации**, определенной **в рамках семейства стандартов ЗИ** комплекса стандартов
РМ.8.2	- **планирование** применения организационных и технических **мер**, направленных на реализацию требований **к процессам системы обеспечения операционной надежности**, определенной **в рамках семейства стандартов ОН** комплекса стандартов

ГОСТ Р 57580.1:

8.2.2 Базовый состав мер планирования процесса системы защиты информации приведен в таблице 48.

(Условное обозначение мер – «ПЗИ»)

ГОСТ Р 57580.4:

8.2.2 Базовый состав мер планирования процесса системы обеспечения операционной надежности приведен в таблице 18.

(Условное обозначение мер – «ПОН»)

Меры, связанные с 57580.1 и 57580.4

Пример 2

Меры	Содержание мер системы управления риском реализации информационных угроз
ЗИУ.3	**Реализация, контроль и совершенствование процессов** системы защиты информации, определяемой в рамках семейства стандартов ЗИ комплекса стандартов, **планирование которых предусмотрено мерой РМ.8.1** таблицы 14
ЗИУ.7	**Реализация, контроль и совершенствование процессов** системы обеспечения операционной надежности, определенной в рамках семейства стандартов ОН комплекса стандартов, **планирование которых предусмотрено мерой РМ.8.2 таблицы 14**

ГОСТ Р 57580.1:

8.3.2 Базовый состав мер по реализации процесса системы защиты информации приведен в таблице 49.

8.4.2 Базовый состав мер контроля процесса системы защиты информации приведен в таблице 50.

8.5.2 Базовый состав мер по совершенствованию процесса системы защиты информации приведен в таблице 52.

(Условные обозначения мер – «РЗИ», «КЗИ», СЗИ»)

ГОСТ Р 57580.4:

8.3.2 Базовый состав мер по реализации процесса системы защиты информации приведен в таблице 19.

8.4.2 Базовый состав мер контроля процесса системы защиты информации приведен в таблице 20.

8.5.2 Базовый состав мер по совершенствованию процесса системы защиты информации приведен в таблице 21.

(Условные обозначения мер – «РОН», «КОН», СОН»)

Классификация событий риска

Классификация событий риска реализации информационных угроз

Примечание: обязательной классификацией для кредитных организаций является приведенная в Приложении 5 к Положению Банка России от 08.04.2022 № 716-П.

Классификация, приведенная в приложении А к ГОСТ Р 57580.3, коррелирует с приложением 5 к Положению БР 716-П, но выходит за его пределы и включает в том числе:

Типы атакуемых объектов (А.7.3):

в) на прикладном уровне объектов информатизации (уровне автоматизированных систем и приложений), используемых клиентом финансовой организации при получении финансовых и (или) информационных услуг:

- **мобильное приложение**;

д) **работники финансовой организации**;

е) **причастные стороны** финансовой организации (за исключением клиентов финансовой организации);

ж) **клиенты финансовой организации**.

Расширение применяемой классификации следует планировать при реализации мер ГОСТ Р 57580.3.

Классификация событий риска

Классификация, приведенная в приложении Б к ГОСТ Р 57580.3 (классификации событий риска ИБ по типам событий), имеет свои особенности.

Кредитные организации при классификации в качестве первого уровня классификации должны применять типы событий операционной риска, установленные нормативными актами Банка России:

- ✓ преднамеренные действия персонала;
- ✓ преднамеренные действия третьих лиц;
- ✓ нарушение кадровой политики и безопасности труда;
- ✓ нарушение прав клиентов и контрагентов;
- ✓ ущерб материальным активам;
- ✓ нарушение и сбои систем и оборудования;
- ✓ нарушение организации, исполнения и управления процессами.

Положение БР 716-П

Раскрывает состав событий, входящих в перечисленные типы событий риска ИБ

Линии защиты

Три линии защиты в рамках управления рисками ИБ

Центры компетенций

- идентификация риска ИБ в рамках реализуемых ими бизнес- и технологических процессов;
- сбор информации и информирование о внутренних событиях риска ИБ и потерях;
- участие в оценке риска ИБ в рамках реализуемых ими бизнес- и технологических процессов;
- обеспечение соблюдения требований к мероприятиям, направленным на уменьшение негативного влияния риска ИБ

Служба управление рисками
Служба ИБ

- интеграция системы управления риском ИБ в систему управления ОР;
- валидация КИР;
- расчет и обоснование сигнальных и контрольных значений КПУР;
- расчет фактических значений КПУР;
- координация деятельности по управлению риском ИБ и отражению информации о событиях риска ИБ в базе событий ОР;
- формирование отчетности об управлении риском ИБ;
- определение согласованной или единой методологии управления риском ИБ

Уполномоченное подразделение

- валидация и верификация методологии, данных;
- валидация внутренней отчетности;
- содействие своевременному и адекватному реагированию на недостатки функционирования системы управления риском ИБ;
- оценка соблюдения требований нормативных актов Банка России

Линии защиты

Три линии защиты в рамках управления рисками ИБ

Центры компетенций

Подразделения, которые:

- осуществляют операции и сделки в рамках своих процессов и несут ответственность за результаты выполнения процесса и за достижение целевых показателей процесса
- обеспечивают процессы финансовой организации

Бизнес подразделения,
Подразделение ИТ

Служба управление рисками
Служба ИБ

Поминим. К рискам ИБ относятся в т.ч. виды риска:

✓Связанные с обработкой (хранением, уничтожением) информации без использования объектов информатизации

✓Побуждение клиентов финансовой организации к осуществлению финансовых (банковских) операций

СУР, СИБ,
Противодействие мошенничеству

Уполномоченное подразделение

Подразделение, независимое от СУР и СИБ которое:

- уполномочено проводить оценку эффективности функционирования системы управления риском ИБ, в т.ч. оценку полноты и качества выполнения мероприятий, направленных на уменьшение негативного влияния от риска ИБ

СВА/СВК

Линии защиты

Три линии защиты в рамках управления рисками ИБ

Центры компетенций

Служба управление рисками
Служба ИБ

Уполномоченное подразделение

Бизнес подразделения,
Подразделение ИТ

СУР, СИБ,
Противодействие мошенничеству

СВА/СВК

Задействованы (интервьюируются) при проведении внешнего аудита

Спасибо за внимание!
Вопросы?

АО «ДиалогНаука»
Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75
E-mail: svintsitskii@dialognauka.ru

http://www.DialogNauka.ru