УТВЕРЖДАЮ
Директор ООО «Файнекс»

_____ А.А. Сташевский
20.06.2023

МЕТОДИКА
управления риском нарушения
информационной безопасности
в ООО «Файнекс»

ГЛАВА 1
Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Методика управления риском нарушения информационной безопасности ООО «Файнекс» (далее – Методика) устанавливает цели, задачи, общую организацию управления рисками нарушения информационной безопасности, а также основные функции органов управления, работников ООО «Файнекс» (далее – Организация), участвующих в указанном процессе.

1.2. Настоящая Методика является элементом общей системы управления Организацией, разработана в соответствии с утвержденным Наблюдательным советом Парка высоких технологий (далее – ПВТ) Положением о требованиях, которым должны соответствовать отдельные заявители для регистрации их в качестве резидентов Парка высоких технологий и Порядком управления рисками в ООО «Файнекс» (далее – Порядок).

1.3. Для целей настоящей Методики нижеприведенные термины используются в следующих значениях:

компоненты информационной системы Организации – серверное оборудование, активное сетевое оборудование, персональные электронно-вычислительные машины, системное и прикладное программное обеспечение;

риск нарушения информационной безопасности (риск нарушения ИБ) – риск, связанный с угрозой нарушения свойств информационной безопасности (доступности, целостности или конфиденциальности) информационных активов Организации, в том числе, киберриск;

киберриск – риск возникновения у Организации потерь (убытков) и (или) дополнительных затрат вследствие противоправных действий сторонних лиц в отношении компьютерных и информационных систем или сетей, систем связи, информационных ресурсов и потоков Организации, совершаемых посредством информационных и телекоммуникационных технологий.

1.4. Иные термины по тексту настоящей Методики используются в значениях, определенных Декретом Президента Республики Беларусь от 21.12.2017 № 8 «О развитии цифровой экономики» и иными нормативными правовыми актами, актами Наблюдательного совета ПВТ, Политикой информационной безопасности (кибербезопасности) ООО «Файнекс».

1.5. В случаях если отдельные нормы настоящей Методики вступят в противоречие с действующим законодательством Республики Беларусь, актами

Наблюдательного совета ПВТ, применению подлежат соответствующие нормы законодательства Республики Беларусь и актов Наблюдательного совета ПВТ до внесения необходимых изменений в настоящую Методику.

1.6. Во всем ином, что не предусмотрено настоящей Методикой, Организация руководствуется законодательством Республики Беларусь, актами Наблюдательного совета ПВТ и иными локальными правовыми актами Организации (далее – ЛПА).

1.7. Актуализация настоящей Методики осуществляется по мере необходимости на основании анализа информации, полученной в рамках мониторинга и оценки риска нарушения ИБ, но не реже одного раза в год.

ГЛАВА 2
ЦЕЛИ, ЗАДАЧИ И ОБЩАЯ ОРГАНИЗАЦИЯ ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ НАРУШЕНИЯ ИБ

2.1. На информационные активы, владельцем которых является Организация и которые вовлечены в технологические и бизнес-процессы, воздействуют внешние и внутренние угрозы, что обуславливает возникновение рисков нарушения ИБ.

2.2. Риски нарушения ИБ заключаются в возможности утраты целостности, конфиденциальности и (или) доступности информационных активов Организации, вследствие чего Организации может быть нанесен ущерб.

2.3. Основной целью процесса управления рисками нарушения ИБ является снижение (предотвращение) ущерба Организации, обусловленного утратой или повреждением информационных активов Организации или их свойств, и в совокупности с иными мерами обеспечение устойчивого функционирования Организации и выполнения задач, определенных Уставом, стратегией развития и иными документами Организации.

2.4. Риски нарушения ИБ являются видом операционного риска Организации, а система управления рисками нарушения ИБ является частью системы управления рисками Организации.

2.5. Объектами системы управления рисками нарушения ИБ являются риски нарушения ИБ, связанные с нарушениями конфиденциальности, целостности и доступности информационных активов Организации.

2.6. Субъектами управления рисками нарушения ИБ, осуществляющими управление рисками ИБ, являются должностные лица Организации в соответствии с Главой 8 настоящего Положения.

2.7. Процесс управления рисками нарушения ИБ включает выявление (идентификацию), измерение (оценку), внутренний мониторинг, контроль, ограничение (снижение) уровня рисков нарушения ИБ.

ГЛАВА 3
ВЫЯВЛЕНИЕ (ИДЕНТИФИКАЦИЯ) РИСКОВ НАРУШЕНИЯ ИБ

3.1. Выявление (идентификация) риска нарушения ИБ – система действий работников Организации, направленных на определение вероятных угроз для деятельности Организации, связанных с нарушением свойств безопасности

информационных активов.

3.2. В процессе выявления (идентификации) рисков нарушения ИБ анализируются угрозы ИБ, которые являются существенными в соответствии с моделью угроз ИБ.

Модель угроз ИБ носит прогнозный характер и разрабатывается на основе имеющейся практики и опыта обеспечения ИБ в Организации и взаимодействующих органов и организаций.

Модель угроз ИБ составляется должностным лицом, ответственным за системное администрирование и информационную безопасность в Организации и подписывается директором Организации.

Для поддержания в актуальном состоянии модель угроз ИБ подлежит пересмотру не реже одного раза в год.

3.3. Угрозы ИБ идентифицируются посредством анализа потенциальных источников угроз ИБ, воздействующих на конкретные типы информационных активов через среду их обработки, по перечню согласно Приложению 1 к настоящему Положению.

3.4. В процессе определения угроз ИБ используются следующие типы информационных активов:

служебная информация ограниченного распространения;

сведения, составляющие коммерческую тайну Организации, ее клиентов и контрагентов;

персональные данные работников Организации, ее клиентов и контрагентов;

иная информация ограниченного распространения.

3.5. Средой обработки информационных активов являются:

линии связи и сети передачи данных;

серверное оборудование и персональные электронно-вычислительные машины;

общесистемное и прикладное программное обеспечение;

файлы данных, базы данных, хранилища данных;

носители информации, в том числе бумажные носители;

помещения, здания, сооружения;

информационные технологические процессы.

3.6. В зависимости от типов информационных активов и (или) среды их обработки осуществляется идентификация высокоуровневых рисков нарушения ИБ и низкоуровневых рисков нарушения ИБ компонентов информационной системы Организации.

3.7. Идентификация высокоуровневых рисков осуществляется в Реестре рисков нарушения ИБ Организации (далее – Реестр рисков), образец заполнения которого приведен в Приложении 2 к настоящему Положению.

3.8. Реестр рисков используется для разработки стратегии обеспечения информационной безопасности и построения системы обеспечения ИБ Организации в целом.

3.9. Идентификация низкоуровневых рисков осуществляется в документах, составленных по результатам проведения мероприятий по

управлению уязвимостями компонентов информационной системы Организации.

ГЛАВА 4
ИЗМЕРЕНИЕ (ОЦЕНКА) РИСКОВ НАРУШЕНИЯ ИБ

4.1. Измерение (оценка) уровня рисков нарушения ИБ представляет собой определение величины (уровня) риска с помощью методов качественной оценки для формирования мотивированного суждения об уровне риска.

4.2. Оценка высокоуровневых рисков осуществляется для каждого информационного актива (группы информационных активов) в виде отдельно взятой или совокупности оценок:

степени возможности реализации угроз ИБ (далее – СВР угроз ИБ) источниками угроз ИБ в результате их воздействия на информационные активы или среду их обработки;

степени тяжести последствий от потери свойств ИБ для рассматриваемых типов информационных активов (далее – СТП нарушения ИБ).

4.3. Оценка СВР угроз ИБ и СТП нарушения ИБ определяются на основе экспертного оценивания должностным лицом, ответственным за системное администрирование и информационную безопасность в Организации с привлечением, при необходимости иных работников, являющихся владельцами информационных активов.

4.4. Основными факторами для оценки СВР угроз ИБ являются:

предполагаемые модели действий источников угроз;

возможная частота реализации угроз;

способы реализации угроз;

сложности при обнаружении угроз;

наличие в Организации организационных, технических и прочих защитных мер.

4.5. Для оценки СВР угроз ИБ используется следующая качественная шкала степеней:

нереализуемая;

минимальная;

средняя;

высокая;

критическая.

4.6. Основными факторами для оценки СТП нарушения ИБ являются:

степень влияния на непрерывность деятельности Организации;

степень влияния на репутацию Организации;

объем финансовых и материальных потерь;

объем финансовых, материальных, людских и временных затрат, необходимых для ликвидации последствий нарушения ИБ;

степень нарушения законодательных требований и(или) договорных обязательств Организации;

степень нарушения требований, регулирующих и контролирующих (надзорных) органов в области ИБ, а также требований нормативных актов ПВТ;

объем хранимой, передаваемой, обрабатываемой, уничтожаемой информации.

4.7. Для оценки СТП нарушения ИБ вследствие реализации угроз ИБ используется следующая качественная шкала степеней:

минимальная;

средняя;

высокая;

критическая.

4.8. Оценивание рисков нарушения ИБ (определение допустимых/недопустимых рисков нарушения ИБ) проводится на основании сопоставления оценок СВР угроз ИБ и оценок СТП нарушения ИБ согласно Приложению 3 к настоящему Положению. Полученные значения рисков нарушения ИБ вносятся в Реестр рисков.

4.9. Общая оценка высокоуровневых рисков нарушения ИБ Организации осуществляется по наиболее критичному уровню риска с учетом применимых защитных (компенсирующих) мер. Например, при наличии в реестре рисков нарушения ИБ Организации хотя бы одного риска со значением «недопустимый», общее значение высокоуровневого риска нарушения ИБ Организации – «недопустимый».

4.10. Пересмотр высокоуровневых рисков осуществляется не реже, чем один раз в год и (или) после значительного изменения среды обработки информационных активов Организации.

4.11. Оценка низкоуровневых рисков осуществляется в соответствии с ЛПА по управлению уязвимостями компонентов информационной системы Организации.

4.12. Оценка низкоуровневых рисков, проводимая для каждого компонента информационной системы по результатам внутренних и внешних сканирований на наличие уязвимостей, осуществляется по шкале оценки рисков, используемой сканером уязвимостей. Как правило, используются значения шкалы оценки рисков «критичный», «высокий», «средний», «низкий». При этом риски, имеющие значения «критичный» и «высокий», являются недопустимыми, а значения «средний» и «низкий» – допустимыми.

4.13. Для компонентов информационной системы Организации, имеющих значения рисков «критичный» и «высокий», могут применяться компенсирующие меры, снижающие уровень риска нарушения ИБ для данного компонента информационной системы Организации до значения «средний» или «низкий».

4.14. Оценка низкоуровневого риска для одного компонента информационной системы Организации осуществляется по наиболее критичному уровню риска с учетом применимых компенсирующих мер.

4.15. Общая оценка низкоуровневых рисков для всех компонентов информационной системы Организации осуществляется по наиболее критичному уровню риска с учетом применимых компенсирующих мер. Например, при наличии хотя бы одного компонента с уровнем риска «критичный» с учетом применения компенсирующих мер, общее значение

низкоуровневого риска – «недопустимый».

4.16.Для обобщенной оценки подверженности Организации рискам нарушения ИБ используется сводный уровень рисков нарушения ИБ.

Сводный уровень рисков нарушения ИБ определяется на основании сопоставления оценок высокоуровневых и низкоуровневых рисков нарушения ИБ согласно Приложению 4 к настоящему Положению.

При определении сводного уровня рисков нарушения ИБ Организации используются значения «высокий», «средний», «низкий».

4.17.При наличии технических возможностей оценка и учет рисков нарушения ИБ может осуществляться в виде электронных таблиц или баз данных.

ГЛАВА 5
МОНИТОРИНГ РИСКОВ НАРУШЕНИЯ ИБ

5.1. Мониторинг рисков нарушения ИБ – постоянное наблюдение за информационными активами, обрабатываемыми в информационной системе Организации и (или) участвующими в информационных и технологических процессах Организации, на предмет их подверженности риску нарушения ИБ.

5.2. Мониторинг рисков нарушения ИБ осуществляется посредством:

анализа источников риска - внутренних и внешних факторов, оказывающих влияние на уровень риска нарушения ИБ;

выявления и анализа тенденций, методов и способов реализации угроз нарушения ИБ источниками риска;

анализа состояния защищенности технологических процессов, а также информационной системы Организации и ее компонентов;

выявления, анализа и регистрации выявленных инцидентов ИБ.

5.3. Выявление и анализ источников риска нарушения ИБ, тенденций, методов и способов реализации угроз нарушения ИБ источниками риска осуществляется на постоянной основе посредством взаимодействия и обмена информацией с:

органами по мониторингу и противодействию компьютерным атакам в кредитно-финансовой сфере;

вендорами программного обеспечения, используемого в Организации;

специализированными организациями в сфере обеспечения ИБ.

5.4. Анализ состояния защищенности технологических процессов, а также информационной системы Организации и ее компонентов осуществляется в рамках реализации:

мероприятий процесса по управлению уязвимостями информационной системы Организации;

мероприятий по текущему анализу функционирования системы информационной безопасности и применяемых защитных мер;

аудитов и проверок информационной безопасности.

5.5. В рамках мониторинга рисков нарушения ИБ применяется система ключевых индикаторов рисков нарушения ИБ.

Перечень ключевых индикаторов риска нарушения ИБ, их пороговые значения приведены в Приложении 5 к настоящему Положению.

В случае превышения указанных пороговых индикаторов в Организации вырабатываются предложения по внесению изменений в систему обеспечения ИБ.

ГЛАВА 6
ОГРАНИЧЕНИЕ УРОВНЯ И ОБРАБОТКА РИСКОВ НАРУШЕНИЯ ИБ

6.1. По недопустимым высокоуровневым и низкоуровневым рискам нарушения ИБ составляется план (планы) мероприятий по обработке недопустимых рисков нарушения ИБ (далее – планы мероприятий).

В планах мероприятий должны быть указаны:

перечень информационных активов и компонентов информационной системы Организации и соответствующих рисков нарушения ИБ, уровень которых является недопустимым;

способы (меры) по снижению недопустимого риска;

ответственные за выполнение указанных мер и сроки их выполнения;

дата реализации мер и подпись ответственного лица.

6.2. Возможными способами (мерами) по снижению недопустимых рисков нарушения ИБ являются:

применение мер контроля (минимизации) риска нарушения ИБ (например, применение средств обеспечения ИБ, установка актуальных версий программного обеспечения, установка обновлений безопасности программного обеспечения), компенсирующих и иных мер;

перенос риска на сторонние организации (например, путем страхования указанного риска);

уход от риска (например, путем отказа от предлагаемых технологий или деятельности, которые приводят к появлению риска);

осознанное принятие риска.

6.3. Ответственным за разработку планов мероприятий является должностное лицо, ответственное за системное администрирование и информационную безопасность Организации.

К разработке планов мероприятий привлекаются заинтересованные работники Организации.

6.4. Планы мероприятий согласуются с заинтересованными структурными подразделениями и утверждаются директором Организации или лицом, им уполномоченным.

6.5. Новые риски нарушения ИБ, возникающие в процессе работы Организации и связанные, как правило, с внедрением новых информационных технологий, докладываются директору Организации должностным лицом, ответственным за системное администрирование и информационную безопасность Организации, включаются в Реестр рисков и, при необходимости, в план мероприятий по обработке недопустимых рисков нарушения ИБ.

ГЛАВА 7
ОТЧЕТНОСТЬ ПО РИСКАМ НАРУШЕНИЯ ИБ

7.1. В рамках процесса по управлению рисками нарушения ИБ должностным лицом, ответственным за системное администрирование и информационную безопасность (системным администратором Организации) составляется отчетная документация, которая представляется директору Организации – по фактам реализации рисков нарушения ИБ и инцидентам ИБ.

7.2. Сведения об организации управления рисками нарушения ИБ, а также оценка рисков нарушения ИБ, включаются в отчет по рискам Организации.

ГЛАВА 8
ФУНКЦИИ ДОЛЖНОСТНЫХ ЛИЦ ПО УПРАВЛЕНИЮ РИСКАМИ ИБ

8.1. Общее руководство системой управления рисками нарушения ИБ в рамках управления операционным риском Организации осуществляет директор Организации.

8.2. Непосредственное управление рисками нарушения ИБ осуществляет должностное лицо, ответственное за системное администрирование и информационную безопасность (системный администратор Организации), который:

вырабатывает предложения по целям, задачам, структуре и методологии системы управления рисками нарушения ИБ Организации, возникшего вследствие преднамеренного деструктивного воздействия со стороны работников Организации и (или) третьих лиц;

осуществляет ведение и актуализацию реестра рисков нарушения ИБ;

совместно с заинтересованными работниками Организации составляет планы мероприятий по обработке недопустимых рисков нарушения ИБ;

вырабатывает предложения по приобретению и использованию программных средств по управлению рисками нарушения ИБ;

вырабатывает предложения по обучению работников Организации по вопросам управления рисками нарушения ИБ;

выполняет иные задачи в рамках требований ЛПА Организации по вопросам управления рисками нарушения ИБ.

Приложение 1
к Методике управления риском нарушения информационной безопасности

ПЕРЕЧЕНЬ
основных источников угроз информационной безопасности

Источник угрозы ИБ	Описание
1. Неблагоприятные события природного, техногенного и социального характера	
1.1. Пожар	Неконтролируемый процесс горения, сопровождающийся уничтожением материальных ценностей и создающий опасность для жизни людей. Возможные причины: поджог, самовозгорание, природное явление
1.2. 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 качества информационных услуг (сервисов)
1.3. Нарушение электропитания	Нарушение или снижение качества электропитания. Возможные причины: техногенная катастрофа, стихийное бедствие, природное явление, террористический акт, пожар и т.п. Возможные последствия: сбои и отказы технических средств
1.4. Нарушение функционирования систем жизнеобеспечения	Сбои и аварии в системах водоснабжения, канализации, отопления
1.5. Социальный инжиниринг	Умышленные действия сторонних лиц, преследующие мошеннические цели, реализуемые посредством обмана, введения в заблуждение работников подразделения. Возможные последствия: ошибки работников, нарушение свойств информационных активов, утрата информационных активов, нарушение непрерывности процессов, снижение качества информационных услуг (сервисов)
2. Зависимость от поставщиков (провайдеров, партнеров, клиентов)	
2.1. Зависимость от партнеров (клиентов)	Зависимость от партнеров заставляет Организацию полагаться на их информационную безопасность, Организация должно быть уверено, что партнер сможет обеспечить должный уровень безопасности, либо учитывать данный источник угроз
2.2. Ошибки, допущенные при заключении контрактов с провайдерами внешних услуг	Неточности и неопределенности в договоре с провайдером внешних услуг, которые могут создавать проблемы в работе заказчика

Источник угрозы ИБ	Описание
2.3. Нарушения договорных обязательств сторонними (третьими) лицами	Невыполнение со стороны третьих лиц взятых на себя обязательств по качеству, составу, содержанию и (или) порядку оказания услуг, поставки продукции и т.д. Например, невыполнение требований внешними пользователями, разработчиками или поставщиками программно-технических средств и услуг
2.4. Ошибки в обеспечении безопасности информационных систем на стадиях жизненного цикла	Ошибки в обеспечении безопасности при разработке, эксплуатации, сопровождении и выводе из эксплуатации информационных систем
2.5. Разработка и использование некачественной документации	Некачественное выполнение документированного описания технологических процессов обработки, хранения, передачи данных, руководств для персонала, участвующего в этих технологических процессах, а также описания средств обеспечения ИБ и руководств по их использованию
2.6. Использование программных средств и информации без гарантии источника	Использование в информационной системе Организации непроверенных данных или нелицензионного ПО
3. Сбои, отказы, разрушения (повреждения) программных и технических средств	
3.1. Превышение допустимой нагрузки	Неумышленное превышение допустимой нагрузки на вычислительные, сетевые ресурсы системы. Выполнение работниками большего объема операций, чем это допускается психофизиологическими нормами. Возможные причины: малая вычислительная и (или) пропускная мощность, неправильная организация бизнес-процессов. Возможные последствия: сбои и отказы технических средств, нарушение доступности технических средств, ошибки персонала, нанесение вреда здоровью
3.2. Разрушение (повреждение), аварии технических средств и каналов связи	Физическое разрушение (повреждение) технических средств (каналов связи) или определенное сочетание отказов их элементов, приводящее к нарушениям функционирования, сопряженным с особо значительными техническими потерями, делающие невозможным функционирование технического средства (канала связи) в целом в течение значительного периода времени. Возможные причины: действие внешних (физический несанкционированный доступ, вредительство, террористический акт, техногенная катастрофа, стихийное бедствие, природное явление, гражданские беспорядки) и (или) внутренних (значительные отказы элементов технических средств) факторов. Возможные последствия: нарушение свойств информационных активов, их утрата, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов)

Источник угрозы ИБ	Описание
3.3. Сбои и отказы программных средств	Нарушение работоспособности программных средств. Возможные причины: недопустимое изменение параметров или свойств программных средств под влиянием внутренних процессов (ошибок) и (или) внешних воздействий со стороны вредоносных программ, оператора и технических средств. Возможные последствия: нарушение свойств информационных активов, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов)
3.4. Сбои и отказы технических средств и каналов связи	Прерывание работоспособности технических средств или невозможность выполнения ими своих функций в заранее установленных границах. Возможные причины: недопустимое изменение характеристик технических средств под влиянием внутренних процессов, сложность технических средств, нехватка персонала, недостаточное техническое обслуживание. Возможные последствия: сбои, отказы программных средств, аварии систем, нарушение доступности информационных активов, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов)
3.5. Нарушения функциональности криптографической системы	Случайное или намеренное неправильное управление криптографическими ключами, криптографическими протоколами и алгоритмами, программно-аппаратными средствами систем криптографической защиты информации, приводящее к потере конфиденциальности, целостности информации, нарушению бесперебойности приема-передачи информации, блокировке функционирования платежных и информационных систем Организации
3.6. Нарушения функциональности архивной системы	Нарушение конфиденциальности и целостности архивных данных и (или) непредоставление услуг архивной системой (нарушение доступности) вследствие случайных ошибок пользователей или неправильного управления архивной системой, а также вследствие физических воздействий на компоненты архивной системы
4. Внутренние нарушители	
4.1. Саботаж	Сознательное неисполнение работниками определенных обязанностей или небрежное их исполнение
4.2. Халатность	Невыполнение или ненадлежащее выполнение персоналом своих обязанностей без злого умысла
4.3. Вредительство	Злоумышленное нанесение персоналом вреда информационным активам. В первую очередь вредительство может быть направлено на технические и программные средства, а также на информационные активы. Возможные последствия: ущерб, вызванный нарушением свойств активов, включая их разрушение и уничтожение

Источник угрозы ИБ	Описание
4.4. Ошибки персонала	Любые несоответствующие установленному регламенту или сложившимся практикам действия персонала, совершаемые без злого умысла. Возможные причины: недостаточно четко определенные обязанности, халатность, недостаточное обучение или квалификация персонала. Возникновению ошибок способствуют отсутствие дисциплинарного процесса и документирования процессов, предоставление избыточных полномочий, использование злоумышленником методов социального инжиниринга к персоналу. Возможные последствия: нарушение конфиденциальности целостности, утрата информационных активов, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов), сбои и отказы технических и программных средств
4.5. Хищение	Совершенное с корыстной целью противоправное безвозмездное изъятие и (или) обращение имущества Организации в пользу злоумышленника или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества. Возможные последствия: нарушение свойств информационных активов, их утрата, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов), прямой (непосредственный) ущерб деятельности подразделения
4.6. Выполнение вредоносных программ и кодов	Внедрение в систему и выполнение вредоносных программ: программных закладок, троянских коней, программных вирусов и червей и т.п. Возможные причины: беспечность, халатность, низкая квалификация персонала (пользователей), наличие уязвимостей используемых программных средств. Возможные последствия: несанкционированный доступ к информационным активам, нарушение их свойств, сбои, отказы и уничтожение программных средств, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов)
4.7. Использование информационных активов не по назначению	Умышленное использование информационных активов Организации в целях, отличных от целей Организации. Возможные причины: отсутствие контроля персонала. Возможные последствия: нехватка вычислительных, сетевых или людских ресурсов, прямой ущерб Организации
4.8. Нарушения персоналом организационных мер по обеспечению ИБ	Несоблюдение персоналом требований внутренних документов, регламентирующих деятельность по ИБ
4.9. Ошибки кадровой работы	Ошибки кадровой работы заключаются в приеме на работу неблагонадежных и (или) неквалифицированных сотрудников, увольнении (перемещении) сотрудников без проведения сопутствующих процедур по обеспечению ИБ, непроведении или нерегулярном проведении тренингов и проверок персонала
5. Внешние нарушители	

Источник угрозы ИБ	Описание
5.1. Действия злонамеренного неавторизованного субъекта	Злоумышленные действия со стороны субъекта из внешней по отношению к области обеспечения ИБ среды. Возможные последствия: разрушение и уничтожение технических и программных средств, внедрение и выполнение вредоносных программ, нарушение свойств, утрата информационных активов и сервисов
5.2. Неконтролируемое уничтожение информационного актива	Неумышленное уничтожение информационных активов. Возможные причины: сбои оборудования, природные факторы и техногенные катастрофы. Возможное последствие: прямой ущерб Организации
5.3. Неконтролируемая модификация информационного актива	Неумышленное изменение информационных активов. Возможные причины: сбои оборудования, природные факторы и техногенные катастрофы. Возможные последствия: нарушение непрерывности выполнения процессов, прямой ущерб Организации
5.4. Несанкционированный логический доступ	Несанкционированный логический доступ неавторизованных субъектов к компонентам подразделения и информационным активам. Возможные причины: компрометация пароля, предоставление пользователям (администраторам) избыточных прав доступа, недостатки (отсутствие) механизмов аутентификации пользователей и администраторов, ошибки администрирования, оставление без присмотра программно-технических средств. Одним из путей получения несанкционированного доступа к системе является внедрение злоумышленником вредоносных программ с целью хищения пароля для входа в систему или получения прав доступа. Возможные последствия: нарушение свойств информационных активов, сбои, отказы и аварии программных и технических средств, нарушение непрерывности процессов и (или) снижение качества информационных услуг (сервисов)
5.6. Несанкционированный физический доступ	Физический несанкционированный доступ неавторизованных лиц в контролируемую зону расположения технических средств и (или) информационных активов. Возможные причины: может осуществляться путем обхода средств контроля физического доступа или использования утраченных (похищенных) средств обеспечения доступа. Возможные последствия: разрушение и уничтожение технических и программных средств, нарушение конфиденциальности, целостности, доступности информационных активов, нарушение непрерывности процессов и (или) снижение качества информационных услуг (сервисов)
6. Несоответствие требованиям надзорных и регулирующих органов, действующему законодательству	

Источник угрозы ИБ	Описание
6.1. Несоответствие внутренних документов действующему законодательству, требованиям регуляторов	Несоответствие деятельности может привести к административным и уголовным санкциям со стороны судебных, надзорных и регулирующих органов в отношении должностных лиц (работников) Организации, вызвать остановку отдельных видов деятельности
6.2. Изменчивость и несогласованность требований надзорных и регулирующих органов, вышестоящих инстанций	Непостоянство, различия и коллизии в содержании требований и (или) порядке их выполнения способны дезорганизовать деятельность подразделения или его отдельных служб, снизить ее эффективность и качество, а при определенных обстоятельствах, затруднить ее осуществление. Способствует размыванию или пересечению зон ответственности исполнителей и служб, манипуляции со стороны ответственных лиц и служб своими правами и обязанностями в ущерб общей деятельности. Приводит к перераспределению ресурсов в пользу той деятельности (зачастую не основной), за несоблюдение требований к которой наказание наиболее ощутимое для Организации (должностного лица)

Приложение 2
к Методике управления риском нарушения информационной безопасности

ОБРАЗЕЦ ЗАПОЛНЕНИЯ РЕЕСТРА РИСКОВ НАРУШЕНИЯ ИБ

Тип информацион-ного актива	Тип объекта среды	Источник угрозы ИБ	Способы реализации угроз ИБ	Используемые защитные меры	Оценка СВР угроз ИБ[1]	Оценка СТП нарушения ИБ[2]	Риск нарушения ИБ[3]
Персональные данные клиентов	Файлы, содержащие персональные данные клиентов	Внутренний нарушитель	Несанкционированное копирование	- реализация ролевой модели доступа к информационным ресурсам информационной системы; - логирование событий прикладного ПО и обращений работников к информационным ресурсам информационной системы; - обучение работников правилам работы в информационной системе и проверка знаний работников	Минимальная	Высокая	Допустимый
			Хищение документов	--//--	Минимальная	Высокая	Допустимый
			Внесение несанкционированных изменений	--//--	Минимальная	Высокая	Допустимый
		Внешний нарушитель	Несанкционированный доступ к информационным ресурсам информационной системы	Реализация комплекса мер и процессов на стадиях жизненного цикла информационной системы, применение средств антивирусной защиты, мониторинга событий системного и прикладного ПО, сегментация сети, межсетевое экранирование и др.	Минимальная	Высокая	Допустимый

[1] В графе «Оценка СВР угроз ИБ» используются значения: нереализуемая, минимальная, средняя, высокая, критическая.
[2] В графе «Оценка СТП нарушения ИБ» используются значения: минимальная; средняя; высокая; критическая.
[3] В графе «Результат оценивания рисков нарушения ИБ» используются значения: допустимый; недопустимый.

Приложение 3
к Методике управления риском нарушения информационной безопасности

Таблица для оценки высокоуровневых рисков нарушения информационной безопасности

СВР угроз ИБ	СТП нарушения ИБ			
	минимальная	средняя	высокая	критическая
Нереализуемая	Допустимый	Допустимый	Допустимый	Допустимый
Минимальная	Допустимый	Допустимый	Допустимый	Недопустимый
Средняя	Допустимый	Допустимый	Недопустимый	Недопустимый
Высокая	Допустимый	Недопустимый	Недопустимый	Недопустимый
Критическая	Недопустимый	Недопустимый	Недопустимый	Недопустимый

Приложение 4
к Методике управления риском нарушения информационной безопасности

Оценка сводного уровня рисков нарушения информационной безопасности

Оценка высокоуровневых рисков	Оценка низкоуровневых рисков	
	допустимый	недопустимый
Допустимый	Низкий	Средний
Недопустимый	Средний	Высокий

Приложение 5
к Методике управления риском нарушения информационной безопасности

ПЕРЕЧЕНЬ
ключевых индикаторов риска
нарушения информационной
безопасности

Наименование ключевого индикатора риска нарушения ИБ	Фактов в квартал
1. Хищение, нарушение целостности и доступности информационных активов Организации и персональных данных клиентов	1
2. Несанкционированное распространение за пределами Организации сведений ограниченного распространения Организации	1
3. Нарушение функционирования автоматизированной системы вследствие преднамеренного деструктивного воздействия со стороны работников Организации и (или) сторонних лиц	1
4. Обнаружение в информационной системе Организации вредоносных программ, не выявленных средствами антивирусной защиты	1