DOI:

ПРОБЛЕМАТИКА ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННЫХ СИСТЕМ КОНСТРУКТОРСКОГО БЮРО

Козунова С.С.,
АО «Федеральный научно-производственный центр «Титан-Баррикады», г. Волгоград
one1100on@gmail.com
Черников Б.В.,
Московский институт электронной техники, г. Москва, г. Зеленоград;
Российский экономический университет им. Г.В. Плеханова, г. Москва
bor-cher@yandex.ru
Черникова Е.А.
Российский экономический университет им. Г.В. Плеханова, г. Москва
lb20062006@yandex.ru

Аннотация: Информационные системы конструкторского бюро – основной инструмент повышения эффективности бизнес-процессов, включающий в состав сервера приложений конструкторского бюро, сервера баз данных, файловый сервер и различные модули. Определены задачи, решаемые такими системами. Представлена структура схемы информационной системы конструкторского бюро, описывающая её принадлежность к корпоративной информационной сети. Проведён комплексный анализ проблематики оценки рисков в информационных системах конструкторского бюро, в результате которого установлено, что до настоящего момента существует не только трудность адаптации методов к анализу и оценки рисков информационных систем конструкторского бюро, но и сложность в получении объективных количественных оценок рисков. Описаны риски, характерные для информационных систем конструкторского бюро. Представлена схема процесса оценки рисков. Проанализированы основные методы, применимые к решению задачи оценки рисков. Выявлены их достоинства и недостатки. В статье рассматриваются разработанные авторами модель влияния рисков на информационную систему конструкторского бюро и модель управления рисками информационных систем конструкторского бюро. Проанализированы частные угрозы информационных систем конструкторского бюро и описаны способы их воздействия.

Ключевые слова: информационная система, конструкторское бюро, оценка рисков, финансовые потери.

Введение

Высокие требования к обеспечению непрерывного функционирования информационных систем (ИС) конструкторского бюро (КБ) обусловлены характером решаемых задач и изменениями корпоративной информационной сети (КИС) КБ. Основное предназначение ИС КБ – обеспечение эффективности процессов проектирования, разработки и согласования конструкторской документации, а также автоматизации бизнес-процессов КБ. Основное направление обеспечения непрерывности и надёжности ИС – анализ и оценка рисков. Актуальность проблемы оценки рисков ИС КБ обусловлена: ИС КБ исследуются сравнительно недавно, существует необходимость рационального выбора средств управления рисками ИС КБ. Для существующих методов оценки рисков характерна низкая адаптивность, так как они не учитывают специфику КБ, при их применении, возникают трудности с анализом информационных потоков ИС КБ и их жизненных циклов. Проблема усугубляется тем, что современное развитие ИС КБ происходит в динамически меняющихся условиях, в которых свою очередь наблюдается значительный рост рисков и дестабилизирующих факторов.

1 Информационные системы конструкторского бюро и их основные риски

ИС КБ являются основным инструментом повышения эффективности бизнес-процессов (БП) КБ [1, 2]. Задачи, решаемые в ИС КБ: автоматизация и роботизация БП КБ, совершенствование технологии ведение конструкторского документооборота, обработка конструкторской и технологической документации, интеграция конструкторской документации с технологической документацией, оптимизация электронного согласования конструкторских проектов и различных технических заданий, ведение базы данных с информацией о структуре и конфигурации изделий, подготовка и генерирование отчётов о ходе работы конструкторских подразделений, обеспечение связи с внешними приложениями (смежные системы классов ERP и MES, СУБД, доступ со стороны внешнего приложения к серверной части ИС КБ и с другими). ИС КБ – многопользовательские распределённые системы, построенные по принципу модульности. Преимущество отдаётся клиент-серверной архитектуре. Как правило, ИС КБ содержат следующие прикладные модули: управление структурой и конфигурацией изделия, архивный, обмен данными, технологический, workflow и ряд других модулей,

автоматизирующих БП КБ. Пример схемы такой ИС КБ представлен на рис. 1. Риск – влияние неопределённости на достижение поставленных целей [3]. Приведём основные риски в соответствии с классификационными признаками. По области подверженности риски ИС КБ делятся на: технический, информационный, бизнес-процессный, организационный и финансовый.

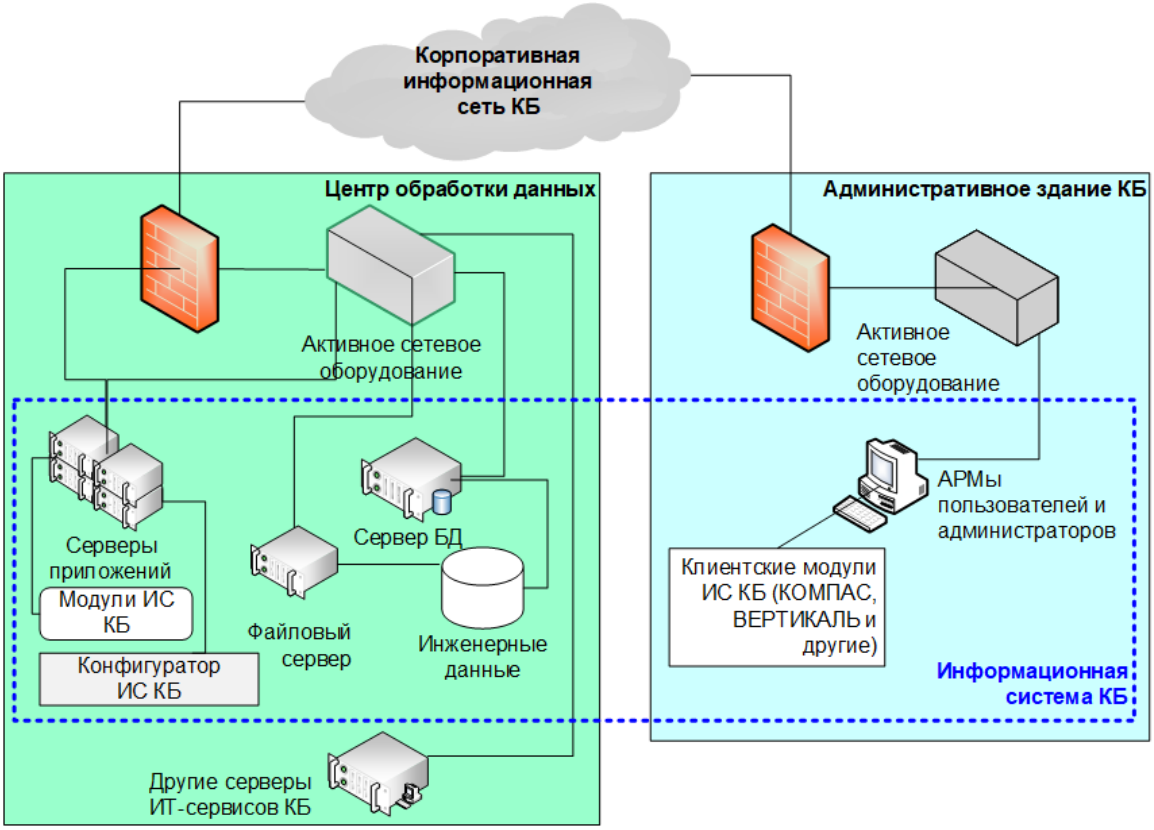

Рис. 1. Пример структуры схемы ИС КБ, функционирующей в корпоративной информационной сети

Информационные риски возникают на уровнях архитектуры систем управления, средств защиты информации, угроз ИС КБ. Бизнес-процессные риски связаны с БП, автоматизируемыми ИС КБ. Организационные риски связаны с недостаточной проработанностью организационных политик КБ, политики информационной безопасности КБ, менеджмента КБ. Технические риски ИС КБ связаны с информационной инфраструктурой, топологии локальной вычислительной сети, программной и аппаратной архитектурами, топологией данных, используемым программным обеспечением, компонентами и модулями ИС КБ. Финансовые риски характеризуются вероятностью потерь финансовых ресурсов (экономические, инвестиционные и другие). По месту возникновения – внутренний и внешний. Внутренние риски связаны со специализацией КБ, внешние – изменение среды, в которой существует КБ (стихийные бедствия, экономическая политика и другое). По степени допустимости риска: допустимый (финансовый ущерб не превышает расчётную сумму прибыли по осуществляемым проектам КБ) и критический (финансовый ущерб исчисляется полной или частичной утратой собственного капитала).

2 Существующие проблемы оценки рисков информационных систем конструкторского бюро

ИС КБ подвержены многочисленным рискам и угрозам. Во избежание получения КБ материального и иного ущерба, который может привести к тяжёлым последствиям (вплоть до значительных репутационных потерь или банкротства КБ), необходимо обеспечивать непрерывное управление рисками ИС [2, 4]. В большинстве КБ отсутствуют процедуры управления рисками и не разработаны мероприятия, снижающие риски и препятствующие их повторному возникновению.

Одна из проблем существующих методов оценки рисков заключается в сложности адаптации этих методов к анализу и оценке рисков ИС КБ, так как они не учитывают специфику КБ, а анализ угроз и ЖЦ ИС КБ является весьма трудоёмкой задачей. Отсюда следует, что для компенсирования

недостатков современных методов, существует необходимость разработки методики оценки и управления рисками ИС КБ, основанной на системном анализе, комплексном подходе и учитывающей информационно – технологические особенности ИС КБ.

Другой, не менее главной проблемой практического применения методов оценки рисков является сложность получения объективных количественных оценок. Величину ущерба рассчитать возможно, но отсутствуют универсальные требования к составу исходных данных, математическим моделям оценки и недостатка статистических данных об угрозах ИС КБ, прогнозирование вероятности наступления риска с приемлемой точностью – весьма трудновыполнимая задача. Такие методы не применимы для оценки рисков ИС КБ, так как не они учитывают программно-информационное и технологическое обеспечение ИС. В основном они применимы для ИС, функционирующих в финансовом секторе.

3 Характеристика процесса оценки рисков

Оценка рисков является процессом и представляет собой совокупность взаимосвязанных действий, преобразующих исходные данные (сведения о рисках) в выходные данные (массив и значение рисков). В соответствии со стандартами [5] и [6] приведём на рис. 2 схему процесса оценки рисков. Оценка рисков применяется на всех стадиях жизненного цикла (ЖЦ) ИС КБ.

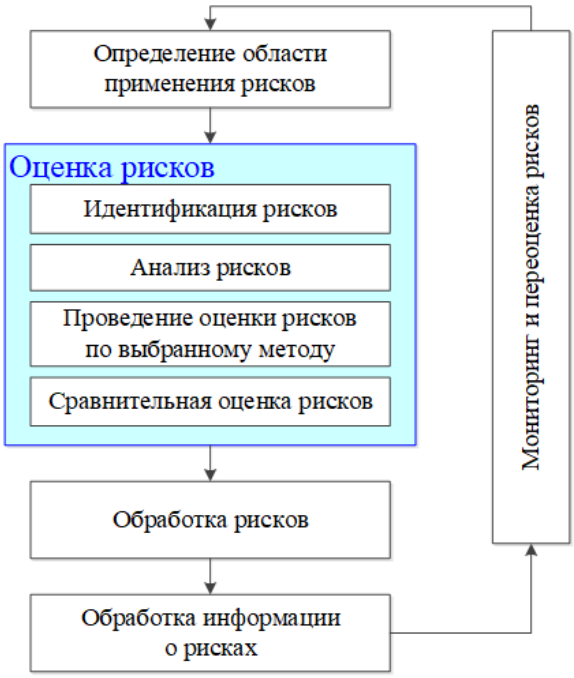

Рис. 2. Схема процесса оценки рисков

В [6] отмечено, что процесс оценки рисков является подпроцессом – частью процесса управления рисками. Идентификация рисков – сбор информации об информационных активах, угроз и ущербов. Анализ рисков определяет характер рисков (источники, последствия, возможности сценариев наступления рисков), и дальнейшие значения параметров: вероятности возникновения рисков, угроз, величины ущерба. Проведение оценки рисков осуществляется в соответствии с алгоритмом выбранного метода. Сравнительная оценка рисков – определение значимости рисков для предприятия и необходимости их последующей обработки. Процесс управления рисками состоит из подпроцессов: установление области применения рисков, обработка рисков, обработка информации о рисках, мониторинг и переоценка рисков.

Установление области применения рисков заключается в определении критериев оценки рисков, границ, области применения управленческого процесса. Обработка рисков заключается в выборе и внедрению мер по модификации факторов рисков. Обработка информации о рисках заключается в достижении договоренности во всех аспектах управления рисками между задействованными сторонами. Мониторинг и переоценка рисков осуществляются для непрерывного контроля рисков и изменения факторов рисков, влияющие на их оценку, ущерб и обработку.

4 Сравнительный анализ методов оценки рисков

Выделяют две основные группы методов оценки рисков: количественная и качественная. Количественная группа методов основывается на анализе процессов ИС [7]. Для оценки факторов риска применяются непрерывные числовые интервалы с помощью экспертных (оценки производятся на непрерывных числовых интервалах экспертным путём) или аналитических (использование данных о частотах, вероятностях возникновения рисков и возможных ущербов) методик [8, 9]. Качественная группа методов позволяет провести экспресс-оценку рисков, ориентированную на определение актуальных рисков ИС [7 - 9]. Оценка рисков осуществляется путём введения качественных шкал и матриц, используемых для оценки факторов и уровней рисков. К количественной группе относятся RiskWatch, IS, метод анализа сценариев [8 - 10]. К качественной – OCTAVE, COBRA, ISO 31000:2018, NIST, BS 7799-3:2017 [8, 9].

Количественные методы обладают следующими особенностями: сконцентрированы на вычислении вероятностей реализации рисков, угроз, ущербов; обладают высокой интерпретируемостью в рамках экономических моделей. К достоинствам этой группы методов следует отнести: возможность формирование оптимальной совокупности управленческих механизмов; возможность формализовано описать процедуру оценки рисков; объективность; прозрачность. В качестве недостатков отметим: ресурсоёмкость; необходимость наличия в КБ высококвалифицированного сотрудника в области анализа рисков; некачественный анализ рисков, некорректная оценка рисков и интерпретация результатов могут привести к избыточности управленческих механизмов и неоправданным затратам. Для качественной группы методов характерны следующие особенности: использует лингвистические значения при оценке последствий наступления рисков. Достоинства качественных методов: простота практического применения; учёт качественного фактора рисков; полученные оценки рисков являются более согласованными, так как используется небольшое количество градаций качественных шкал. Недостатки качественных методов: экспресс-оценка рисков может быть поверхностной из-за отсутствия анализа процессов, происходящих в ИС; трудно проанализировать полученные оценки по причине того, что оценка рисков в рамках одной градации не различается. Наиболее предпочтительным в практическом применении является использование методов количественной оценки рисков [8].

5 Управление рисками информационных систем конструкторских бюро

Так как ИС КБ являются отдельным классом ИС и обладают определёнными особенностями, то процесс управления рисками таких систем имеет некоторые отличия от процесса, характерного для ИС в целом. Модель влияния рисков на ИС КБ представим на рис. 3 схемой со связями, отображающими зависимости между объектами модели.

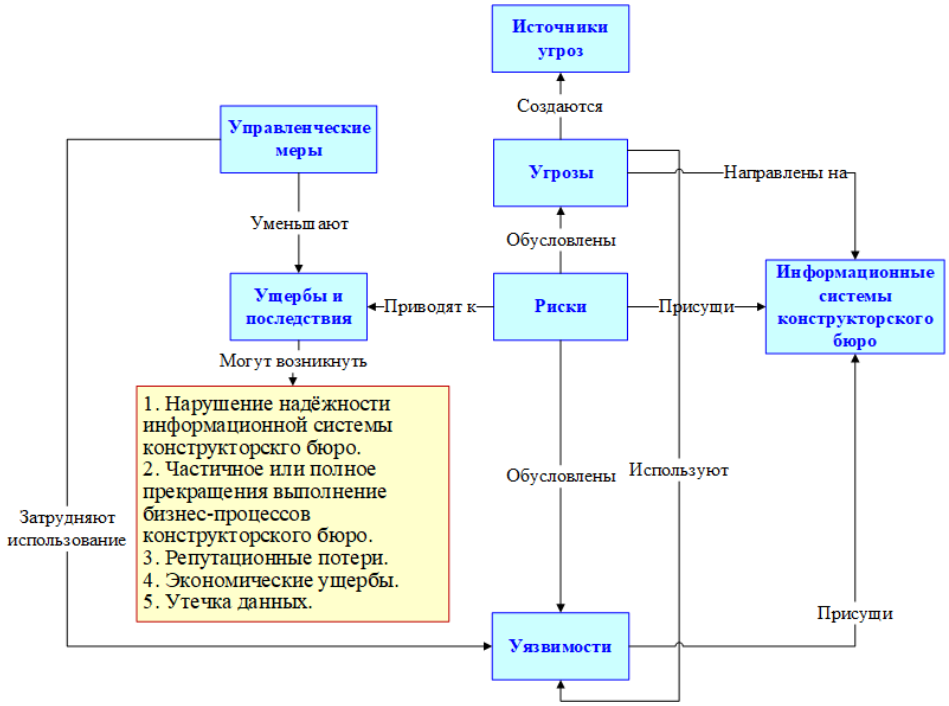

Рис. 3. Модель влияния рисков на информационную систему конструкторского бюро

Таким образом, модель влияния рисков на ИС КБ включает в себя следующие объекты: риски, угрозы, источники угроз, уязвимости, ущербы и последствия, управленческие меры, ИС КБ. Отсюда можно сделать вывод, что анализ угроз ИС КБ является важной задачей при оценке и управления рисками ИС КБ. Совокупность управленческих мер и деятельность, организованная на их основе, образуют систему управления рисками [2, 8].

Модель управления рисками ИС КБ (рис. 4), соответствует процессам менеджмента, которые описываются в [6]. Управление рисками ИС КБ – итеративный процесс, позволяющий детализировать каждую последующую операцию (подпроцессы управления рисками).

6 Анализ угроз в информационных системах конструкторского бюро

При установлении области применения рисков в ИС КБ базовым является выявление факторов рисков. Поскольку риски обуславливаются наличием угроз в ИС КБ, необходимо проводить не только анализ рисков, но и угроз ИС КБ. При разработке модели угроз следует начинать с анализа угроз, способа их воздействия на ИС КБ. В соответствии с [11, 12] анализ угроз позволяет получить сведения об актуальности угроз и соотношению управленческих мер.

Угрозы ИС делятся на следующие виды:

- угрозы, не связанные с деятельностью человека (стихийные бедствия и природные явления);
- угрозы социально-политического характера (саботаж, конфликты и другие);
- угрозы техногенного характера (отключения электропитания, системы заземления, разрушения инженерных сооружений, неисправности аппаратных средств);
- угрозы нарушения конфиденциальности информации; угрозы нарушения целостности информации или программно-аппаратных средств КИС;
- угрозы нарушения доступности информации или программно-аппаратных средств КИС; угрозы утечки по техническим каналам.

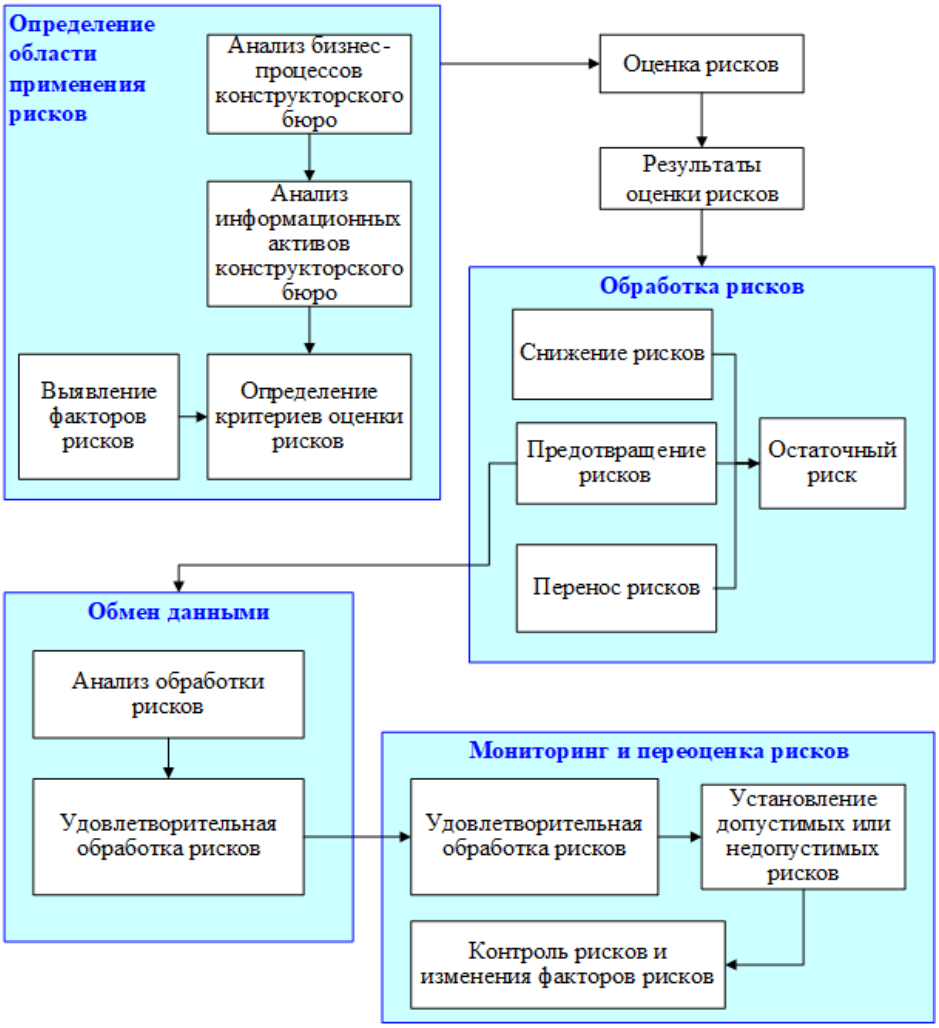

Рис. 4. Модель управления рисками информационных систем конструкторского бюро

Отметим, что наряду с базовыми угрозами, ИС КБ могут быть подвержены другим – частным угрозам. Угрозы, характерные для ИС КБ, и описание способа их воздействия на ИС КБ представлены в таблице 1.

Таблица 1. Угрозы информационных систем конструкторского бюро

Угроза	Способ воздействия
Несанкционированный доступ к информации, обрабатываемой в ИС КБ	Проникновение с использованием уязвимостей ИС КБ, программного обеспечения, протоколов межсайтового взаимодействия
Модификация, уничтожение, блокировка информации, обрабатываемой в ИС КБ	Несанкционированное внесение изменение в информацию, которая обрабатывается в ИС КБ или хранится в базе данных ИС КБ
Нарушение работоспособности ИС КБ	Внесение неисправностей в аппаратные или программные компоненты ИС КБ
Несанкционированное восстановление информации	Анализ содержимого носителей информации, систем хранения данных или баз данных на предмет выявления технико-эксплуатационных характеристик КИС КБ или ИС КБ, данных о профилях пользователей КИС КБ и о системе организации доступа к информации
Несанкционированный доступ к информационным активам КБ	Самовольное изменение или фальсификация прав доступа и полномочий с целью получения возможности обработки данных
Нарушение надёжности ИС КБ	Прерывание функционирования ИС КБ, коммутационного оборудования, каналов связи КИС КБ
Активация уязвимостей программных средств КИС КБ	Попытки эксплуатации уязвимостей ИС КБ, архитектуры ИС КБ или КИС КБ, конфигураций программного обеспечения или технических средств, используя недостатки ИС КБ для негативного воздействия на функционирование такой системы
Перехват информации, передаваемой из ИС КБ и принимаемой в КИС КБ	Проведение анализа сетевого трафика и сканирование сетевых протоколов КИС КБ
Несанкционированное введение в нештатный режим работы ИС КБ	Попытки создания условий для наступления нештатных режимов функционирования ИС КБ, намеренный вывод ИС КБ из отказоустойчивого функционирования
Навязывание ложного сетевого маршрута	Попытки подмена таблиц сетевой адресации КИС КБ
Подбор паролей	Попытки подбора аутентификационных атрибутов для доступа к ресурсам КИС КБ и сервисам ИС КБ
Заражение ИС КБ или КИС КБ вредоносным программным обеспечением	Распространение вирусного программного обеспечения в КИС КБ, попытки прерывания функционирования средств, препятствующих распространению вируса

В исследованиях [2, 7 - 9] отмечено, что угрозы нарушения конфиденциальности информации, обрабатываемой в ИС КБ и целостности информации или программно-аппаратных средств КИС КБ приводят к возникновению рискам, которые наносят наибольший ущерб, иные угрозы – к среднему ущербу.

Заключение

1. Исходя из особенностей ИС КБ и специфики КБ сформированы основные риски ИС КБ. Своевременный анализ и адекватная оценка рисков, а также их предупреждение позволяют обеспечить непрерывность и надёжность функционирования ИС КБ, а также спрогнозировать и, возможно, снизить финансовые потери КБ.
2. Анализ количественных и качественных методов оценки рисков показал, что наиболее предпочтительным в практическом применении является использование методов количественной оценки рисков. Это связано с тем, что такая оценка основана на анализе процессов ИС. Однако существуют следующие ограничения в использовании рассмотренных

методов оценки рисков к ИС КБ: отсутствие системного подхода, сложность анализа рисков, угроз и жизненных циклов ИС КБ, невозможность динамической переоценки рисков при изменении входных данных.

3. Существует необходимость разработки унифицированной комплексной методики оценки рисков ИС КБ.
4. В ходе анализа процесса оценки рисков выявлено, что он является подпроцессом процесса управления рисками. Процесс оценки рисков разделяется на этапы: идентификация, анализ, оценка, сравнительная оценка рисков.
5. Установлено, что управление рисками ИС КБ основано на объектах таких как риски, угрозы, источники угроз, уязвимости, ущербы и последствия, управленческие меры, ИС КБ. Отсюда можно сделать вывод, что одной из задач при оценке и управления рисками является анализ угроз ИС КБ.
6. Разработана модель влияния рисков на ИС КБ, описывающая зависимости между угрозами, ущербами, уязвимостями ИС КБ.
7. В результате анализа угроз ИС КБ выявлено, что помимо типовых угроз ИС для ИС КБ характерны частные угрозы, связанные с надёжностью и непрерывным функционированием ИС КБ, способами обработки информации в ИС КБ, уязвимостями ИС КБ. Установлена взаимосвязь между рисками, угрозами и ущербами, которым может подвергнуться КБ (высокий, средний).

Литература

1. *Шурыгин В.А., Серов В.А., Ковшов И.В., Устинов С.А.* О создании отечественного оборудования для подводной добычи углеводородов // Тр. 14-й Межд. конф. и выставки по освоению ресурсов нефти и газа Российской Арктики и континентального шельфа стран СНГ (CIS Offshore 2019) (г. Санкт-Петербург, 1-4 октября 2019 г.). – СПб: ХИМПРОМ, 2019. С.75-80.
2. *Козунова С.С., Кравец А.Г.* Анализ угроз ЛОЦМАН:PLM в конструкторском бюро // Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта (CAD/CAM/PDM – 2018) : тр. XVIII междунар. молодёжной конф. (г. Москва, 16-18 октября 2018 г.). – М.: ИПУ РАН, 2018. С.328-330.
3. ГОСТ Р 51897-2011. Менеджмент риска. Термины и определения. – М.: Стандартинформ, 2019.
4. *Черников Б.В., Трофимова А.В.* Критериальная система оценки защищённости документов на основе технологии лексикологического синтеза // Современные наукоемкие технологии. 2019. №3-2. С.266-273.
5. ISO 31000:2018 Краткий обзор и ключевые изменения [Электронный ресурс]. – Режим доступа: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/risk/russian/iso-31000-presentation.pdf (дата обращения: 20.06.2020).
6. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – М: Стандартинформ, 2011 г.
7. *Сакрутина Е.А.* Алгоритм оценки рискового потенциала развития технологического процесса на энергоблоке АЭС на основе технико-экономических показателей // Труды 12-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD’2019, Москва). – М.: ИПУ РАН. 2019. С.878-882.
8. *Аникин И.В.* Методы оценки и управления рисками информационной безопасности в корпоративных информационных сетях: моногр. – Казань: Редакц.-издат. центр «Школа». 2015. 224 с.
9. *Астахов А.* Информационная безопасность как искусство управления рисками. – Режим доступа: http://xn----7sbab7afcqes2bn.xn--p1ai/content/soderzhanie (дата обращения: 18.06.2020).
10. *Изотова А.Р., Федоров В.М.* Методический подход к оценке рисков информационной безопасности предприятия // ЭКОНОМИНФО. 2018. Т.15, №2. С.82-90.
11. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. Зам. директора ФСТЭК России 14 февраля 2008 г. [Электронный ресурс]. – Режим доступа: https://fstec.ru/component/attachments/download/290 (дата обращения: 20.06.2020).
12. Банк данных угроз безопасности информации ФСТЭК России [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/threat (дата обращения: 20.06.2020).