РОЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ РИСКОВ ПРЕДПРИЯТИЯ

Кремчеева Лилия Ренатовна

студент, Санкт-Петербургский государственный архитектурно-строительный университет, РФ, г. Санкт-Петербург

Дурандина Анна Павловна

научный руководитель, канд. экон. наук, доцент, Санкт-Петербургский государственный архитектурно-строительный университет, РФ, г. Санкт-Петербург

THE ROLE OF INFORMATION SECURITY IN THE ENTERPRISE RISK SYSTEM

Lilia Kremcheeva

Student, St. Petersburg State University of Architecture and Civil Engineering, Russia, St. Petersburg

Durandina Anna Pavlovna

scientific advisor, candidate of economic sciences, associate professor, St. Petersburg State University of Architecture and Civil Engineering, Russia, St. Petersburg

Аннотация. В данной статье рассматривается роль информационной безопасности в системе рисков предприятия. Составлена классификация рисков коммерческого предприятия. Проанализирована статистика по утечкам конфиденциальной информации.

Abstract. This article discusses the role of information security in the enterprise risk system. A classification of risks of a commercial enterprise has been developed. Analyzed statistics on confidential information leaks.

Ключевые слова: информация, информационная безопасность, экономическая безопасность, риск.

Keywords: information, information security, economic security, risk.

Один из основоположников кибернетики Норберт Винер считал, что «Информация – это не материя и не энергия, информация – это информация» [4]. Особенное положение информации как явления создало огромное количество определений.

В соответствии с ГОСТ 33707-2016 (ISO/IEC 2382:2015) «Информационные технологии» информация (в области обработки информации) – любые данные, представленные в электронной форме, написанные на бумаге, высказанные на совещании или находящиеся на

любом другом носителе, используемые финансовым учреждением для принятия решений, перемещения денежных средств, установления ставок, предоставления ссуд, обработки операций и т. п., включая компоненты программного обеспечения системы обработки [2].

В свою очередь в концепции обеспечения информационной безопасности информацией являются сведения, которые доступны для сбора, хранения, обработки, использования и передачи различными способами, в том числе в компьютерных сетях и других информационных системах. Такие сведения обладают высокой ценностью и могут стать объектами посягательств со стороны третьих лиц. Стремление оградить информацию от угроз лежит в основе создания систем информационной безопасности.

В аспекте экономической безопасности информационную безопасность следует понимать, как понятие защищенности предприятия и ее информационных ресурсов от неблагоприятного воздействия деструктивных обстоятельств, обеспечивающие целостность ключевых элементов информации, а также результата становления социально-экономических показателей предприятия.

Термины «экономическая безопасность», «информационная безопасность» и определение «риск» были введены не так давно в источниках научной информации, но неразрывно связаны в обсечение безопасности на предприятиях. Поэтому следует определить базовые понятия этих терминов. Экономическая безопасность представляет собой процесс непрерывного обеспечения на предприятии стабильности функционирования, защиты от неблагоприятного воздействия факторов, рисков внешней и внутренней среды, в том числе возможности улучшения на различных этапах функционирования [5].

Поскольку в аспекте экономической безопасности предприятия не содержится единого подхода к определению «риск», следует обратиться к одному из авторов современной научной литературы. Е. Н. Безверхая рассматривает риск как «угрозу утраты предприятием части своих ресурсов (финансовых, интеллектуальных и др.), появления непредвиденных расходов и недополучения доходов вследствие осуществления производственной и финансовой деятельности» [3].

Существует множество рисков, характерных для коммерческих предприятий, и количество постоянно растет, на сегодняшний день дано описание более 220 видов, поэтому следует их классифицировать. Единой классификации рисков не существует. Как отмечает М. А. Рогов, такое наблюдается из-за тесной взаимосвязи и замещения рисков.

Одним из первых классификацией рисков занялся Дж. М. Кейнс, подошедшего к данному вопросу со стороны субъекта, осуществляющего инвестиционную деятельность, подчеркнув три основных вида рисков: предпринимательский риск, риск «заимодавца», риск изменения ценности денежной единицы. Также концепцией классифицирования рисков работали такие ученые как Н. Б. Ермасова, С. В. Ермасов, И. Н. Шапкин, М. А. Рогов, Ю.М Бахрамов, В. В. Глухов.

Опираясь на труды вышеупомянутых авторов, составим свою классификацию рисков коммерческого предприятия.

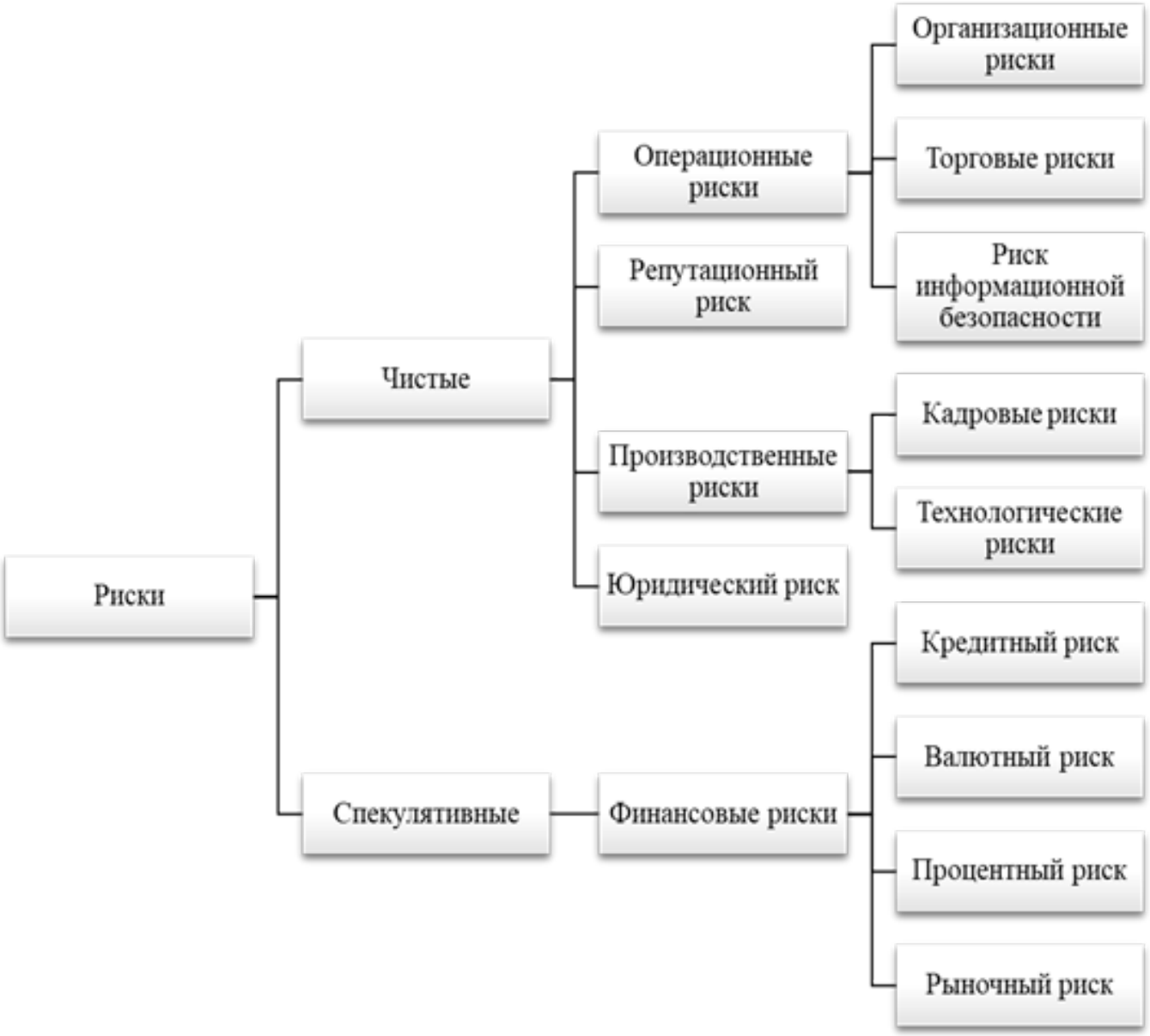

Рисунок 1. Классификация рисков коммерческого предприятия

Из классификации рисков видно, что риск информационной безопасности относится к операционным рискам. Операционный риск — риск убытка в результате неадекватных или ошибочных внутренних процессов, действий сотрудников и систем или внешних событий. Отсюда следует, что предприятие, при реализации рисков информационной безопасности, может понести экономические потери, например, прямые денежные потери при краже активов; репутационный ущерб; потеря клиентов; критическая остановка производства, угрожающая невосполнимым нарушением непрерывности бизнеса; утрата конкурентного преимущества вследствие утечки конфиденциальных данных; штрафы за несоответствие требованиям регуляторов в области информационной безопасности и другие.

В декабре 2016 года Указом Президента Российской Федерации № 646 утверждена Доктрина информационной безопасности Российской Федерации. В документе информационная безопасность представлена как положение защищенности национальных интересов в информационной сфере. В данном случае национальные интересы представляют собой совокупность интересов общества, личности и государства, каждая группа интересов необходима для стабильного функционирования социума [1].

Правоотношения, связанные с обеспечением информационной безопасности, регулируются:

- Закон РФ от 21.07.1993 N 5485–1 «О государственной тайне»;
- Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»;
- Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Банк данных угроз безопасности информации – ФСТЭК России;
- Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации.

На основе вышеупомянутых нормативных актов подготавливаются новые постановления правительства и ведомственные нормативные акты, предназначенные актуальным вопросам обеспечения защиты информации. Перед тем, как разрабатывать стратегию информационной безопасности, целесообразно принять ключевой термин данного понятия, который позволит использовать поставленный набор методов, а также способов защиты.

Научные деятели в области защиты информации дают понятие термина «информационная безопасность», как устойчивое состояние защищенности информации, ее носителей и инфраструктуры, гарантирующая целостность и устойчивость процессов, относящиеся к информации, к умышленным или непреднамеренным воздействиям естественного и искусственного характера.

Влияния подразделяются в качестве угроз информационной безопасности, наносящие потери элементам информационных отношений. Информационная безопасность в данном случаи выступает одной из особенностью функционирования системы. Поэтому система всегда должна владеть определенным уровнем защищенности, осуществляющимся на каждом временном отрезке в период деятельности системы. Следует также обратить внимание на статистику по утечкам информации (рис. 2)

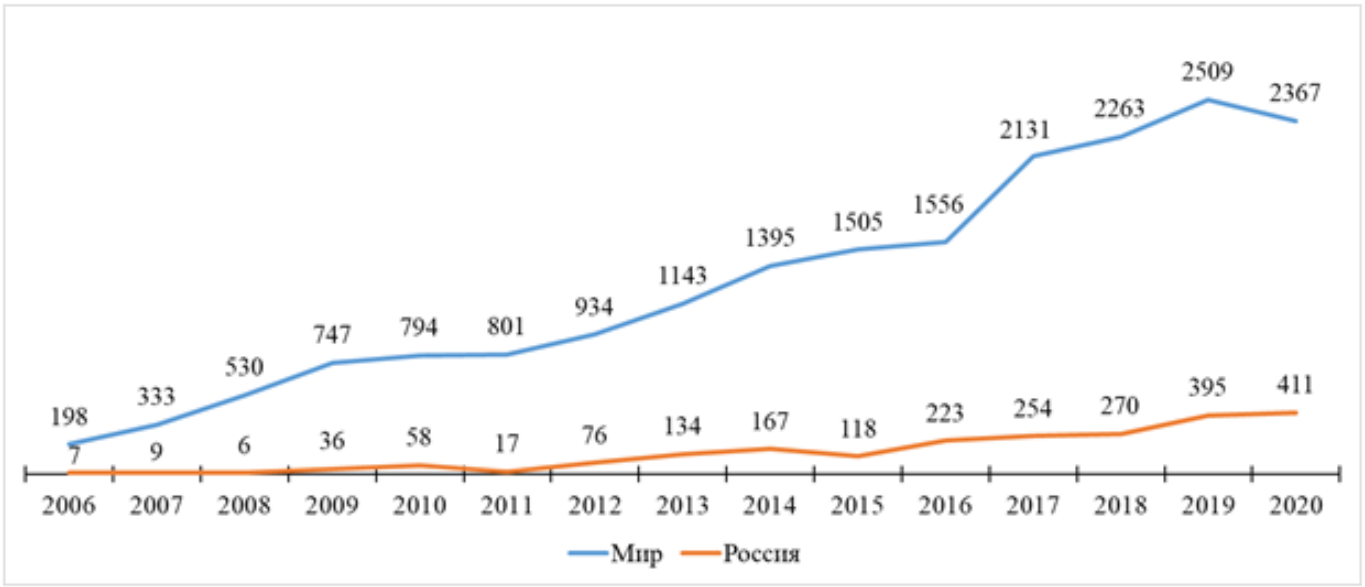

Рисунок 2. Число зафиксированных утечек информации, Мир – Россия, 2006–2020 гг

В 2020 году в мировом «рейтинге» государств, потерпевших утечки информации, Российская Федерация занимает второе место с результатом в 15,7 %, первое место – США. Объем скомпрометированных данных, который пришелся на российские компании и государственные организации, не превысил 1,1% от совокупного объема данных, скомпрометированных по всему миру.

Субъектами информационной безопасности являются владельцы и пользователи информации, при этом пользователями считаются не только сотрудники организаций, которые на регулярной основе соприкасаются с информацией, но и пользователи, использующие базы данных в редких случаях, к примеру, муниципальные органы, запрашивающие нужную им информацию.

Поддерживающая инфраструктура, с точки зрения основ информационной безопасности, включает компьютеры, сети, телекоммуникационное оборудование, помещения, системы жизнеобеспечения, персонал. При анализе безопасности следует рассмотреть каждый элемент системы, также отдельно изучить персонал организации, так как в большинстве случаев именно по вине сотрудников происходит утечки информации (рис. 3).

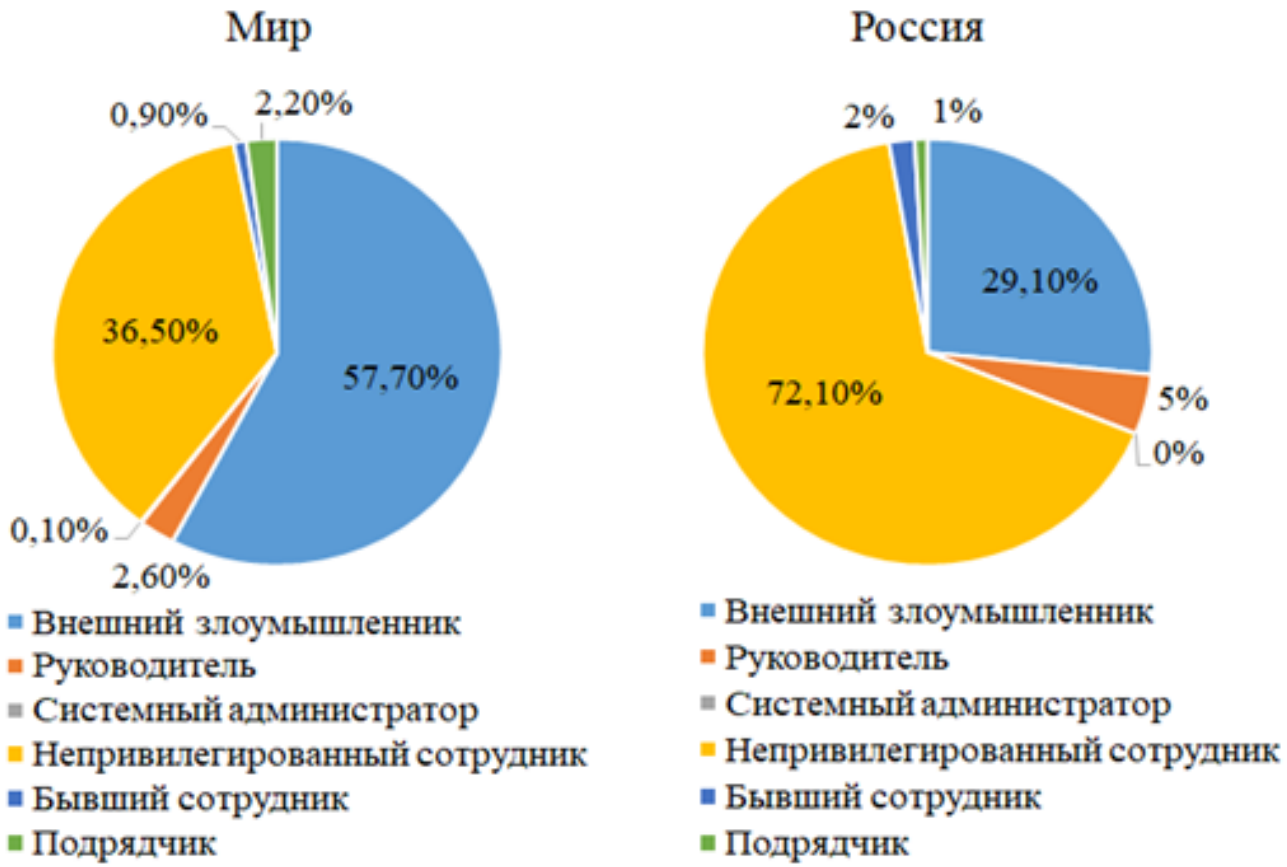

Рисунок 3. Распределение утечек информации по виновнику, Мир – Россия, 2020 год

Анализ статистики по 2020 году показал, что среди виновных лиц утечки информации в России вдвое меньше, чем в мире, нарушений от внешних нарушителей (неизвестных лиц или хакеров). В Российской Федерации преобладает нарушения персонала организации.

Таким образом, информационную безопасность в системе рисков предприятия следует понимать, как совокупность административных, организационных, правовых и технических мер, ориентированных на устранение и предотвращение существующих либо вероятных угроз информационной безопасности. Постоянство процесса защиты информации гарантирует противодействие угрозам на каждой стадии информационного цикла, включающий процесс сбора, хранения, обработки, использования и передачи информации.

Список литературы:

1. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». // Собрании законодательства Российской Федерации от 12 декабря 2016 г. N 50 ст. 7074.

2. ГОСТ 33707-2016 (ISO/IEC 2382:2015) Информационные технологии (ИТ). Словарь. – М.: Стандартинформ, 2016.

3. Безверхая Екатерина Николаевна, Губа Ирина Игоревна, Ковалева Ксения Александровна Экономическая безопасность предприятия: сущность и факторы // Научный журнал КубГАУ. 2015. №108.

4. Винер Н. Кибернетика, или управление и связь в животном и машине; или Кибернетика и общество/ 2-е издание. — М.: Наука; Главная редакция изданий для зарубежных стран, 1983. — 344 с.

5. Кривякин К. С., Изотова А. Р., Федоров В. М. Методический подход к оценке рисков информационной безопасности предприятия // ЭКОНОМИНФО. 2018. №2.