Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Высшая школа электроники и компьютерных наук
Кафедра «Защита информации»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2020 г.

Оценка рисков информационной безопасности автоматизированной системы в организации

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.03.01.2020.160.ПЗ ВКР

Руководитель проекта,
д.п.н., профессор
_____ Л.В. Астахова
_____ 2020 г.

Автор проекта,
студент группы КЭ-407
_____ И.А. Сафонова
_____ 2020 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2020 г.

Челябинск 2020

АННОТАЦИЯ

Сафонова И.А. Оценка рисков информационной безопасности автоматизированной системы в организации – Челябинск: ЮУрГУ, КЭ-407, 145 с., 7 ил., 12 табл., библиогр. список – 41 наим., 7 прил.

Выпускная квалификационная работа выполнена с целью разработки методики оценки рисков информационной безопасности организации и ее документационное обеспечение, методического обеспечения практикума для изучения оценки рисков информационной безопасности в вузе.

В выпускной квалификационной работе отражены все этапы создания оценки рисков информационной безопасности, от исследования нормативных документов до заключения о результатах эффективности практических работ.

В процессе выполнения квалификационной работы было проведено исследование нормативно-правовых документов, методик и программных продуктов для оценки рисков. Были разработаны: методика оценки рисков информационной безопасности организации и шаблоны для документирования, методическое обеспечение практикума для изучения оценки рисков информационной безопасности в вузе.

ОГЛАВЛЕНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций [4].

Актив – все, что имеет ценность для организации [8].

Банковская система Российской Федерации (БС РФ) – Банк России, кредитные организации, а также представительства иностранных банков [26].

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [5].

Информация – сведения (сообщения, данные) независимо от формы их представления [29].

Информация, составляющая коммерческую тайну – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны [31].

Информационная безопасность – состояние защищенности интересов в условиях угроз в информационной сфере [6].

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [29].

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств [30].

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [29].

Менеджмент риска – скоординированные действия по руководству и управлению организацией в отношении риска [9].

Оценка риска информационной безопасности организации – общий процесс идентификации, анализа и определения приемлемости уровня риска информационной безопасности организации [6].

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [30].

Риск информационной безопасности – возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации [9].

Система менеджмента информационной безопасности (СМИБ) – часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности[8].

Снижение риска – действия, предпринятые для уменьшения вероятности, негативных последствий или того и другого вместе, связанных с риском [9].

Сохранение риска – принятие бремени потерь или выгод от конкретного риска [9].

Угроза – возможная причина нежелательного инцидента, который может нанести ущерб системе или организации [7].

Уязвимость – слабое место актива или меры и средства контроля и управления, которое может быть использовано угрозой [7].

ВВЕДЕНИЕ

Информация всегда была и остается ценным ресурсом. С развитием информационных технологий, информация стала обрабатываться, передаваться и храниться в электронном виде. В настоящее время сложно представить организацию, не обладающую конфиденциальной информацией. Но с обладанием такого ресурса приходит и риск нарушения конфиденциальности, целостности, доступности, что может привести к финансовым трудностям, а возможно и к разрушению репутации компании.

Изначально оценка рисков большего всего применялась в экономической, экологической, политической и военной сферах деятельности. О рисках в области информационной безопасности всерьез заговорили лишь в конце XX века. Управление рисками в области защиты информации имеет свои специфические особенности. Однако стоит отметить, что многие положения теории рисков информационной безопасности берут свое начало из общей теории рисков. Сейчас у оценки рисков существуют свои стандарты, методики и даже программные продукты, которые помогают специалисту в измерении, принятии решений о расстановке приоритетных действий и не только.

Основной задачей оценки рисков является объективная идентификация и оценка наиболее значимых для бизнеса информационных рисков организации, а также проверка адекватности используемых мер и средств защиты информации.

Любая организация обладающая информацией, которая интересна большому количеству пользователей или имеющая серьезную конкуренцию на рынке, хоть раз задумывалась об оценке рисков. Чем больше компания, тем больше риски, поэтому оценка рисков информационной безопасности в нашей стране присуща банковской и нефтегазовой сферам. Такие компании применяют специальные программные решения для автоматизации процесса управления. Но что если организация не готова вкладывать крупные финансовые ресурсы для внедрения оценки рисков? В таком случае этот процесс полностью ложится на плечи специалиста по защите информации в организации. В ходе, которого он должен раз-

работать и внедрить ряд документов для оценки рисков, провести ее и зафиксировать результаты.

Предметом выпускной квалификационной работы является оценка рисков информационной безопасности автоматизированной системы организации.

Целью дипломной работы является разработка методики оценки рисков информационной безопасности организации и ее документационное обеспечение, а также разработка методического обеспечения практикума для изучения оценки рисков информационной безопасности в вузе.

В соответствии с поставленной целью необходимо решить следующие задачи:

1) исследовать нормативно-правовые документы;
2) исследовать существующие методологии и программные продукты оценки рисков, провести их сравнительный анализ;
3) исследовать способы оценки рисков, применяемые организациями;
4) разработать методику оценки рисков информационной безопасности организации и ее документационное обеспечение;
5) разработать методическое обеспечение практикума для изучения оценки рисков информационной безопасности в вузе.