Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.45+004.056

Казберович
Игорь Геннадьевич

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ОЦЕНКИ УЯЗВИМОСТЕЙ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

АВТОРЕФЕРАТ
на соискание степени магистра

по специальности 1-98 80 01 Информационная безопасность

Научный руководитель
Власова Галина Александровна
кандидат технических наук,
доцент кафедры ЗИ, БГУИР

Минск 2021

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Информатизация является одним из способов увеличения эффективности функционирования предприятия. Большинство бизнес-процессов на предприятии подвергаются автоматизации, например, бухгалтерия, логистика, человеческие ресурсы кампании, управление взаимоотношениями с клиентами и прочие. С целью повышения эффективности работы, предприятия приобретают корпоративные информационные системы, которые позволяют вывести управление бизнес-процессами на новый уровень. В свою очередь информационные системы собирают и обрабатывают огромное количество конфиденциальных данных за сохранность и доступность которых беспокоится руководство предприятия. Поскольку любая информационная система имеет ряд уязвимостей, которыми могут пользоваться нарушители, требуется проводить работы по определению уязвимостей и снижению рисков их эксплуатации угрозами. Одним из способов для своевременного выявления и предотвращения рисков является опрос сотрудников на предмет наличия такого рода уязвимостей. Таким образом, проблема защиты данных в рамках корпоративных информационных систем является актуальной на сегодняшний день.

В настоящее время активно используется ряд методологий для оценки рисков, одними из наиболее распространённых являются:

- CRAMM;
- OCTAVE;
- CORAS;
- RiskWatch.

В работе рассматриваются роль управления рисками информационной безопасности стандарты, подходы к оценке рисков, руководства по менеджменту рисков, анализ и сравнение вышеперечисленных методологий.

Целью работы является разработка программного обеспечения по оценке уязвимостей корпоративных информационных систем.

Предмет исследования – методологии и инструментальные средства оценки уязвимостей.

Решение о разработке своего программного обеспечения было принято на основании того, что в настоящее время не существует методологии, покрывающей ряд актуальных уязвимостей корпоративных информационных систем и являющейся бесплатной.

Для достижения поставленной цели предусмотрено решение следующих задач:

1. Изучить роль управления рисками информационной безопасности в организации и подходы к оценке рисков информационной безопасности.

2. Исследовать стандарты и руководства по менеджменту рисков информационной безопасности.

3. Провести сравнительный анализ ряд популярных методологий оценки рисков.

4. Разработать программного обеспечение на основе созданной методологии оценки уязвимостей корпоративных информационных систем.

5. Провести опрос сотрудников с помощью метода CRAMM и разработанной методологии, проанализировать полученные результаты.

ОБЗОР ЛИТЕРАТУРЫ

В источниках [1-3] представлено управление рисками информационной безопасности и способы их минимизации.

В работе [4] авторы описывают методики и технологии управления информационными рисками.

В источниках [5-8] содержится информация об информационных рисках при внедрении информационных систем.

В работе [9] авторы описывают критерии и процессы управления рисками.

В источниках [10-13] содержится информация об управлении информационными рисками, их анализе и оценке.

В работе [14] автор приводит классификацию угроз информационной безопасности.

В источниках [15-16] предлагается информация по основам управления информационной безопасностью.

В источнике [17] приводится информация о проверке и оценке деятельности по управлению информационной безопасностью.

В источнике [18] описывается управление инцидентами информационной безопасности и непрерывностью бизнеса.

В источниках [19-20] описываются основные подходы к анализу и оценке рисков информационной безопасности, а также методы оценки и управления рисками информационной безопасности в корпоративных информационных сетях.

В источниках [21-32] описаны международные стандарты ISO, государственные стандарты СТБ и национальный стандарт РФ ГОСТ.

В источниках [33-35] объясняется экономическая целесообразность информационной безопасности.

В источнике [36] представлен отчет по анализу защищенности корпоративных информационных систем, выполненных в 2018 году специалистами Positive Technologies. Документ содержит обзор наиболее распространенных недостатков безопасности, практические примеры их эксплуатации и описание вероятных векторов атак, а также рекомендации по повышению уровня защищенности.

В источниках [37-40] представлены методологии управления ИТ-рисками, а также значение обеспечения информационной безопасности в области управления рисками бизнеса.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе приводятся общие сведения по роли управления рисками информационной безопасности в организации и подходы к оценке рисков информационной безопасности. Организация использует реактивный и проактивный подходы для взаимодействия с рисками. Что касается оценки рисков, то существует качественная, количественная оценка и смешанный подходы. Применение конкретного подхода оценки рисков зависит как от сферы деятельности организации (например, в банковской сфере может применяться более строгий количественный анализ), так и от стадии жизненного цикла системы (например, на начальных этапах цикла может проводиться только качественная оценка рисков, а на более зрелых - уже количественная).

Во второй главе приводится анализ стандартов и руководств по менеджменту рисков информационной безопасности, среди которых ISO 27001:2013, ISO/IEC 27002:2013, ISO/IEC 27005:2018, СТБ 34.101.70-2016, ГОСТ Р 56546-2015, NIST SP 800-30 "Guide for Conducting Risk Assessments".

В третьей главе описана автоматизация процесса управления рисками. Автоматизация процессов управления рисками позволяет повысить эффективность работы за счёт осуществления качественного и прозрачного управления рисками организации, снижения влияния человеческого фактора, повышения культуры управленческих рисков и уровня корпоративного управления. Для более подробного сравнения были выбраны одни из наиболее популярных методологий: CRAMM, OCTAVE, CORAS и RiskWatch. Выделены достоинства и недостатки каждой из методик, сформированы требования, которые должны быть учтены в разрабатываемой методологии оценки уязвимостей корпоративных информационных систем.

В четвертой главе приведено обоснование метода оценки уязвимостей информации, обрабатываемой в корпоративных информационных системах. Сформирован перечень уязвимостей корпоративных информационных систем, на основании которых должны строится вопросы в разрабатываемой методологии.

В пятой главе описана реализация программного обеспечения по оценке уязвимостей корпоративных информационных систем и сравнение результатов анализа с методологией CRAMM. Программное обеспечение представлено в виде сайта, выполненного с использованием HTML, Bootstrap и jQuery. Проведены опросы сотрудников организации и выполнено сравнение разработанной методологии и CRAMM методологии. Приведены угрозы, которые могут использовать уязвимости, приведенных в разработанной методологии. Исходя из анализа выше, расхождения в результатах опроса по разработанной методологии и CRAMM методологии связано с игнорированием некоторых уязвимостей, а также с чрезмерным усложнением вопросов касательно ряда уязвимостей в CRAMM. Разработанное программное обеспечение на основе методологии оценки уязвимостей корпоративных информационных систем покрывает ряд недостатков рассматриваемых

методологий (CRAMM, OCTAVE, CORAS, RiskWatch), выявленных в процессе анализа. Разработанное программное обеспечение предоставляет простоту и удобство использования, требует минимальных финансовых и временных затрат для ответов на представленные вопросы, а также упрощает прохождение опроса сотрудниками, не имеющими технической квалификации, и главное выявляет уязвимости актуальные для корпоративных информационных систем малых и средних предприятий.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В ходе выполнения работы были достигнуты все поставленные цели. Согласно поставленным целям были исследованы стандарты и руководства по менеджменту рисков информационной безопасности, проведен сравнительный анализ популярных методологий оценки рисков таких как CRAMM, OCTAVE, CORAS, RiskWatch, разработана методология по оценке уязвимостей корпоративных информационных систем и, как результат, разработано программное обеспечение на основе данной методологии. Также выполнен сравнительный анализ результатов опроса сотрудников организации с помощью разработанной методологии и CRAMM.

Путем анализа стандартов по менеджменту рисков информационной безопасности, а также выявления достоинств и недостатков каждой из проанализированных методологий были сформированы требования к разрабатываемому программного обеспечению.

На данный момент существует множество методологий и соответствующего программного обеспечения по выявлению и оценке рисков информационной безопасности, однако они имеют ряд недостатков. Некоторые из них покрываются методиками частично либо чрезмерно усложнены, в разрабатываемом программном обеспечении учтены обнаруженные анализом недостатки, кроме этого в основу разрабатываемого ПО положены следующие принципы:

- покрытие ключевых уязвимостей корпоративных информационных систем;
- простота и удобство использования ПО;
- минимальные временные затраты для ответов на представленные вопросы;
- не требуется технической квалификации сотрудников;
- минимальные финансовые затраты на ПО;
- подходит для малых и средних организаций;

Разработанное программное обеспечение позволяет оценить риски ряда ключевых уязвимостей корпоративных информационных систем и своевременно предпринять действия по их выявлению, что ведет к обеспечению целостности, доступности и конфиденциальности информации, обрабатываемой в рамках корпоративных информационных систем.

Тестирование методом опроса сотрудников организации показало, что программное обеспечение справляется со своей задачей.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Власова Г.А., Казберович И.Г. Агрегированный анализ рисков / Г.А. Власова, И.Г. Казберович // Управление информационными ресурсами: материалы XVI Международной научно-практической конференции, Минск, 26 февр. 2020 г. / Академия управления при президенте Республики Беларусь; редкол.: Н.Л. Бондаренко. – Минск, 2020. – С. 213–214.
2. Казберович И.Г. Практики минимизации информационных рисков в организациях / И.Г. Казберович // Инфокоммуникации: материалы: 56-я юбилейная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 18-20 мая 2020 г. / БГУИР, Минск, Беларусь: тезисы докладов. – Мн. – 2020. С. 23-24
3. Казберович И.Г. Оценка уязвимостей корпоративных информационных систем методом опроса сотрудников организации / И.Г. Казберович // Управление информационными ресурсами: материалы XVII Международная научно-практическая конференция «Управление информационными ресурсами», Минск, Академия управления, 12.03.2021 / Академия управления при президенте Республики Беларусь; тезисы докладов. – Минск, 2021. – С. 213–214.