АНАЛИЗ ПОДХОДОВ К АУДИТУ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Бурькова Е.В., Хрыкина Н.А.
Оренбургский государственный университет, г. Оренбург

Защита персональных данных на современном этапе развития информационного общества приобретает все большую значимость. Это связано с проникновением информационных технологий во все сферы нашей жизни, человек становится частью интернет-пространства, он окружен интеллектуальными мобильными устройствами, повсеместным видеонаблюдением; в организациях и фирмах практически все процессы обработки персональных данных автоматизированы. Возможности для сбора, хранения и обработки информации расширяются и становятся доступными для широкого круга лиц [5]. В этих условиях становится целесообразным осуществление регулярного аудита защищенности персональных данных, обрабатываемых в информационных системах. Аудит защищенности ИСПДн направлен на обеспечение прав и свобод человека и гражданина при обработке его персональных данных, общественных и государственных интересов, соблюдения законных интересов лиц, использующих персональные данные в своей деятельности, укрепления правовой защищенности и безопасности личности граждан Российской Федерации.

Аудит защищенности проводится с целью установления степени выполнения требований по обеспечению состояния защищенности ИСПДн. Результаты аудита могут указывать на соответствие или несоответствие критериям аудита или указывать на принятие мероприятий по модернизации системы защиты ПДн организации. Суть аудита сводится к оценке защищенности ИСПДн.

Согласно ГОСТ Р ИСО 19011-2012 «Руководящие указания к аудиту систем менеджмента», процедура оценки защищенности проводится как в «ручном» режиме так и в автоматизированном с привлечением специальных программных комплексов оценки защищенности и рисков, реализующих различные методики.

При проведении анализа литературы по этой теме были выделены следующие подходы к аудиту защищенности ИСПДн: формальный, классификационный, категорированный, количественные оценки рисков, качественные оценки защищенности, комплексные оценки защищенности ИС. Наиболее распространены количественный и качественный походы к аудиту защищенности информационных систем.

На основе анализа источников [1,2,4] была построена классификация подходов к аудиту защищенности ИС, представленная на рисунке 1.

Рисунок 1 – Классификация подходов к аудиту защищенности ИСПДн

В количественном подходе для описания риска используется двухмерная характеристика: степень риска и цена риска. Степень риска количественно характеризует вероятность негативных результатов принятого решения. Цена риска дает количественную характеристику вероятных потерь.

Количественная оценка рисков применяется в ситуациях, когда исследуемые угрозы и связанные с ними риски можно сопоставить с конечными количественными значениями ущерба, выраженным в деньгах, процентах, времени, человеко-ресурсах.

Подход количественной оценки защищенности информационных систем включает в себя:

– экспертные оценки информационной безопасности, в основе которых лежит понятие профиля защиты стандарта ISO/IEC 15408. ГОСТ Р ИСО/МЭК 15408 определяет «Общие критерии», которые предназначены для использования в качестве основы при оценке характеристик безопасности средств и систем информационных технологий;

– построение модели нарушителя и модели угроз для предприятия;

– алгоритм распределения функций безопасности с учетом всех видов информационных потоков, находящихся в оцениваемой ИС (защита от внешних воздействий (со стороны Интернета), защита от внутренних атак);

– графовый метод оценки защищенности;

– анкетирование субъектов отношений, которые служат для уяснения направленности деятельности предприятия, предполагаемых приоритетов целей безопасности, задач, решаемых ИС и эксплуатации ИС. [4]

Сущность графового метода оценки защищенности состоит в построении оценки защищенности объектов на основе характеристик защитных механизмов (ЗМ) для этого объекта и определении достаточности системы ЗИ.

Объект исследования представляется в виде графа, вершинами которого являются «модули защиты» и защищаемые объекты, а связи – это возможные пути продвижения нарушителя. Модуль защиты – это некоторый конечный результат разложения системы защиты, который можно представить в виде элемента задержки. Таким образом, получившийся граф позволяет проследить возможные пути продвижения «нарушителя» к защищаемому объекту. Вершина графа, характеризующая «модуль защиты», обладает временем задержки, имеет выходы (ребра графа). Вероятность всех выходящих из одной вершины ребер равна единице.

Количественная оценка цены риска может определяться абсолютным или относительным уровнем потерь. В абсолютном выражении риск может определяться величиной возможных потерь в физическом (натурально-вещественном) или стоимостном (денежном) выражении. В относительном выражении риск определяется как отношение величины возможных потерь к некоторой базе, например, капиталу, суммарным издержкам или прибыли.

При качественном подходе не используются количественные или стоимостные выражения для объекта оценки. Вместо этого объекту оценки присваивается показатель, проранжированный по трехбалльной), пятибалльной или десятибалльной шкале (низкий, средний, высокий). Для сбора данных при качественной оценке рисков применяются опросы целевых групп, личные встречи. Качественный подход к аудиту защищенности ИСПДн реализован в программе оценки рисков «Гриф». [3]

Подход качественной оценки систем анализа защищенности ИС организации включает:

– сбор и изучение исходных данных по ИС;

– оценку рисков, связанных с осуществлением угроз безопасности в отношении средств предприятия;

– анализ политики безопасности предприятия и организационно-распорядительной документации по обеспечению ИБ

– оценка организационно-распорядительной документации соответствия требованиям существующих нормативных документов;

– тестирование систем ИБ включает в себя проверку эффективности механизмов защиты и поиск уязвимостей. [2]

Анализ рисков начинается с формализации системы приоритетов организации в области ИБ. Для оценки ценности ресурсов необходимо выбирать подходящую систему критериев. Критерии должны позволять описать потенциальный ущерб, связанный с нарушением конфиденциальности, целостности, доступности. Анализ рисков информационной безопасности качественным методом должен проводиться с привлечением сотрудников, имеющих опыт и компетенции в той области, в которой рассматриваются угрозы.

Тестирование системы защиты проводится для проверки эффективности используемых в ней защитных механизмов, их устойчивости к атакам, а также с целью поиска уязвимостей. Традиционно используются два основных метода тестирования: по методу «черного ящика» и по методу «белого ящика». Тестирование по методу «черного ящика» предполагает отсутствие у тестирующей стороны каких-либо специальных знаний о конфигурации и внутренней структуре объекта испытаний. Против объекта испытаний реализуются все известные типы атак.

Метод «белого ящика» предполагает составление программы тестирования на основании знаний о структуре и конфигурации объекта испытаний. В ходе тестирования проверяется наличие и работоспособность механизмов безопасности, соответствие состава и конфигурации системы защиты требованиям безопасности и существующим рискам. Выводы о наличии уязвимостей делаются на основании анализа конфигурации используемых средств защиты и системного программного обеспечения, а затем проверяются на практике.

Количественная оценка позволяет определить числовое выражение вероятности возникновения рисков и их влияние на проект.

Нами был проведен сравнительный анализ подходов, результат которого представлен в таблице 1. Каждый из подходов имеет свои преимущества и недостатки, сложность и особенности реализации, а также форму представления показателя общей защищенности систем.

Таблица 1 – Сравнительная характеристика подходов к аудиту защищенности

Наименование подхода	Преимущества	Недостатки
Качественная оценка систем ИБ	Простота применения. Применимость для прогнозирования практически любых ситуаций. Выявление качественного соответствия или несоответствия системы ИБ определенным требованиям, проверка	Не применяется в условиях неполной информации. Практическая реализация данного подхода является затруднительной.
Количественный подход к аудиту защищенности	Показывает характеристики существующих механизмов защиты на исследуемой ИС, определяет достаточность системы защиты информации. Степень риска количественно характеризует вероятность негативных результатов принятого решения. Цена риска	Отсутствуют гарантии, что полученные в результате опроса экспертов данные достоверны. Существуют трудности в проведении опроса экспертов и

	дает количественную характеристику вероятных потерь.	обработке полученных результатов

Таким образом, в результате проведенной работы была дана характеристика подходов к аудиту защищенности, проанализированы подходы к аудиту защищенности. Количественный подход к аудиту защищенности более выгоден в применении, ввиду практичности и преимуществ, превосходящих в количестве положительные характеристики качественной оценки. Аудит ИСПДн является эффективным инструментом для получения данных о текущем уровне защищенности от угроз информационной безопасности и позволяет повысить уровень защищенности ИСПДн.

Список литературы

1. *Бурькова, Е.В. Задача оценки защищенности информационных систем персональных данных / Е.В. Бурькова // Вестник Чувашского университет. – Чебоксары, 2016. - № 1. – С. 112-118. ISSN: 1810-1909*

2. *Методика оценки рисков информационной безопасности [Электронный ресурс]: Контур – Электрон. журн. – Москва, 2015. – Режим доступа: https://kontur.ru/articles/1691 (дата обращения: 11.12.2016).*

3. *Современные методы и средства анализа и управление рисками информационных систем компаний [Электронный ресурс]: Безопасность как искусство – Электрон. журн. – Москва, 2015. – Режим доступа: https://dsec.ru/ipm-research-center/article/modern_methods_and_means_for_ analysis_and_risk_management_of_information_systems_of_companies/ (дата обращения: 05.12.2016).*

4. *Кондаков С.Е. К вопросу о количественной оценке защищенности информации от несанкционированного доступа в информационных системах [Электронный ресурс] / Кондаков С.Е. // Труды Международного симпозиума «Надежность и качество» – Электрон. дан. – Пенза, 2015. – С. 83-85.*

5. *Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2015 год [Электронный ресурс]: Роскомнадзор – Электрон. дан. – Москва, 2015. – Режим доступа: http://rkn.gov.ru/docs/Otchet_ZPD_rus2015.pdf (дата обращения: 12.12.2016).*