Сиротюк В.О.

Анализ и оценка рисков информационной безопасности организаций

Аннотация: В работе рассмотрены задачи построения эффективной системы информационной безопасности организаций, возникающие на этапе предпроектного анализа и исследования систем управления организациями. Рассмотрены уязвимые элементы и угрозы информационной безопасности и описаны их характеристики. Разработаны методы анализа и оценки рисков информационной безопасности. Предложенные подходы и методика позволяют повысить эффективность разработки и внедрения системы управления информационной безопасностью организаций.

Ключевые слова: информационная безопасность, система управления информационной безопасностью, объект защиты, угроза информационной безопасности, риск информационной безопасности, уязвимый элемент

Введение

Централизация хранения информационных ресурсов и активов организаций в базах данных (БД) центров обработки данных (ЦОД) и децентрализация их использования пользователями выдвигают проблему обеспечения требуемого уровня защиты данных от преднамеренного или непреднамеренного несанкционированного доступа, модификации или разрушения данных.

Высокий уровень безопасности данных может быть достигнут разработкой и внедрением формализованных моделей и методов анализа и синтеза оптимальных механизмов и системы защиты структур БД и создаваемой на их основе системы управления информационной безопасностью (СУИБ) организации [1].

Создание эффективной СУИБ организации носит комплексный характер, что требует для ее решения сочетания законодательных, нормативно-правовых, организационных, программных и технических мер. Важно то, что СУИБ является частью бизнес-процессов организации и должна быть встроена в общую структуру управления организации, и, таким образом, вопросы

информационной безопасности (ИБ) учитываются при разработке процессов, информационных систем и средств управления ими. СУИБ направлена на сохранение конфиденциальности, целостности и доступности информации за счет применения процессов управления рисками и обеспечивает уверенность руководства организаций в том, что риски ИБ надлежащим образом выявляются, классифицируются, анализируются, контролируются и по ним оперативно принимаются контрмеры.

В работе определены основные уязвимые элементы и угрозы информационной безопасности организаций и описаны их характеристики, предложены методы анализа и оценки рисков ИБ.

Основные угрозы информационной безопасности и уязвимые элементы ресурсов и объектов защиты

Основными угрозами ИБ являются [1, 2]:

- раскрытие конфиденциальной информации (несанкционированный доступ, копирование данных, кража информации),
- компрометация информации (внесение несанкционированных изменений в массивы данных и БД),
- несанкционированный обмен информацией,
- отказ от информации (непризнание получателем или отправителем фактов получения или отправки информации, соответственно),
- отказ в обслуживании (отсутствие доступа к информации).

Основные уязвимые элементы ресурсов и объектов защиты в организации приведены в таблице 1.

Таблица 1 – Уязвимые элементы объектов защиты организаций

Объекты и ресурсы	**Уязвимые элементы**
Оборудование	процессор, клавиатура, терминал, рабочая станция, принтер, коммуникационные линии, серверы, маршрутизаторы
Программы	тексты программ, объектные модули, утилиты, диагностические программы, операционные системы

Объекты и ресурсы	Уязвимые элементы
Данные	оперативные, архивные, резервные копии, журнальные записи, базы данных, передаваемые через сеть
Люди	пользователи, администраторы, группа поддержки оборудования
Документы	на программы, оборудование, системы, административные процедуры
Материалы	фонды, бумага, формы, ленты, магнитные и электронные носители

Принципиально возможными путями утечки информации в организации могут быть:

- прямое хищение носителей информации и документов,
- копирование конфиденциальной информации,
- несанкционированное подключение к терминалу пользователей и незаконное его использование для доступа к информации,
- несанкционированный доступ к данным с помощью специальных программных средств.

На рисунке 1 представлена классификация возможных угроз безопасности, которая не является исчерпывающей. Полное множество уязвимых элементов и угроз безопасности выявляется в ходе выполнения предпроектных работ по обследованию и анализу систем управления организациями и информационных систем.

Методы анализа и оценки рисков информационной безопасности организаций

Организация должна регулярно проводить оценку рисков нарушения информационной безопасности.

Процесс оценки рисков ИБ должен удовлетворять следующим требованиям [2]:

- гарантировать непротиворечивость, обоснованность и сопоставимость результатов оценки рисков ИБ;

- обеспечивать выявление рисков ИБ, включая процесс оценки рисков ИБ, направленный на идентификацию рисков, связанных с

потерей конфиденциальности, целостности и доступности информации в рамках области действия СУИБ;

- обеспечивать определение источников риска;
- обеспечивать анализ рисков ИБ;
- обеспечивать оценку рисков ИБ. Оценка рисков включает в себя выполнение процедур сравнения результатов анализа рисков с критериями риска и ранжирование рисков по приоритетам для последующей их обработки.

Рисунок 1 – Классификация угроз безопасности

Организация должна сохранять данные по оценке рисков информационной безопасности документально.

Анализ рисков ИБ позволяет идентифицировать имеющиеся угрозы, оценить вероятность их успешного осуществления, возможные последствия для организации и правильно расставить

приоритеты при реализации контрмер. По результатам анализа разрабатывается система первоочередных мероприятий по уменьшению величины рисков до приемлемого уровня.

Процесс анализа и оценки рисков включает в себя выполнение следующих групп задач [2, 3]:

- анализ ресурсов, включая информационные ресурсы, программные и технические средства, людские ресурсы, и построение модели ресурсов, учитывающей их взаимозависимости;
- анализ задач, решаемых информационными системами, позволяющий оценить критичность информационных ресурсов, с учетом их взаимозависимостей;
- идентификация угроз безопасности в отношении ресурсов информационной системы и уязвимостей защиты, делающих возможным осуществление этих угроз;
- оценка вероятности осуществления угроз, величины уязвимостей и ущерба, наносимого ведомству;
- определение величины рисков для каждой тройки: угроза – группа ресурсов – уязвимость;
- ранжирование существующих рисков.

Для каждого вида ресурсов необходима своя методика определения ценности элементов, помогающая выбрать подходящий набор критериев. Эти критерии служат для описания потенциального ущерба, связанного с нарушением конфиденциальности и достоверности информации, уровня ее доступности. Физические ресурсы оцениваются с точки зрения стоимости их замены или восстановления работоспособности. Эти стоимостные величины затем преобразуются в ранговую (качественную) шкалу, которая используется также и для информационных ресурсов. Программные ресурсы оцениваются тем же способом, что и физические, на основе определения затрат на их приобретение или восстановление.

Для оценки рисков ИБ может использоваться следующая формула:

$$R=D*P(V),$$

где R — риск информационной безопасности;

D – критичность актива (ущерб);

P(V) – вероятность реализации уязвимости.

Одним из примеров практической реализации вышеописанного подхода к определению уровней риска является матрица рисков, приведенная в таблице 2.

Таблица 2 – Матрица рисков (согласно рекомендациям NIST "Risk Management Guide for Information Technology Systems")

Угроза (ее вероятность)	Ущерб		
	(низкий) — 10	*(средний) -50*	*(высокий) -100*
(высокая) — 1	(низкий) 10x1=10	(средний) 50x1=50	(высокий) 100x1=100
(средняя) — 0.5	(низкий) 10x0.5=5	(средний) 50x0.5=25	(средний) 100x0.5=50
(низкая) — 0.1	(низкий) 10x0.1=1	(низкий) 50x0.1=5	(низкий) 100x0.1=10
Уровень риска: Высокий (от 50 до 100); Средний (от 10 до 50); Низкий (от 1 до 10)			

Заключение

В условиях возрастающих рисков и угроз информационной безопасности организаций, обусловленных применением злоумышленниками все более изощренных методов и средств промышленного шпионажа, направленных на взлом систем защиты ЦОД, раскрытие, подмену, модификацию и искажение информации БД обеспечение ИБ и защиты информационных ресурсов, информационной и обеспечивающей инфраструктуры организаций является важной и актуальной задачей. Ее решение позволит организациям обеспечить конфиденциальность, достоверность, целостность, доступность и сохранность БД.

В работе рассмотрены основные уязвимые элементы и угрозы информационной безопасности организаций, определены возможные пути утечки информации, приведена классификация возможных угроз безопасности.

Основное внимание уделено рассмотрению требований, описанию процесса, а также методики анализа, оценки и обработки рисков ИБ организаций. С этой целью предложена формула для оценки рисков ИБ. Полученные результаты используются в

дальнейшем при построении оптимальной СУИБ организации. Предложенные подходы и методы использовались при построении системы информационной безопасности международной региональной патентной организации – Евразийского патентного ведомства Евразийской патентной организации, повышении эффективности и качества патентных информационных фондов [3].

Данная работа подготовлена в рамках программы Президиума РАН № 30 (7) «Теория и технологии многоуровневого децентрализованного группового управления в условиях конфликта и кооперации»

Литература:

1. *Кульба В.В., Ковалевский С.С., Косяченко С.А., Сиротюк В.О.* Теоретические основы проектирования оптимальных структур распределенных баз данных. Серия «Информатизации России на пороге XXI века». – М.: СИНТЕГ, 1999. – 660 с.

2. *Кульба В.В., Сиротюк В.О., Косяченко С.А.* Информационная безопасность патентных ведомств: теория и практика. – М.: ИПУ РАН, 2017. – 166 с.

3. *Кульба В.В., Сиротюк В.О.* Формализованная методология повышения эффективности и качества патентных информационных фондов и опыт ее использования при формировании и развитии евразийского патентно-информационного пространства. – М.: ИПУ РАН, 2019. – 236 с.

Козлов А.Д., Нога Н.Л.

Построение модели оценки риска информационной безопасности с использованием метода нечеткой логики

Аннотация: Предложен вариант построения модели оценки риска информационной безопасности с использованием метода нечеткой логики.

Ключевые слова: риск, оценка риска, модель, информационная безопасность, нечеткая логика

В современном обществе происходит стремительный процесс цифровизации всех сфер жизнедеятельности человека: все больше услуг предоставляется в цифровом (электронном) виде, торговля