АНАЛИЗ УЯЗВИМОСТЕЙ КАК КЛЮЧЕВОЙ ЭТАП ПРОЕКТИРОВАНИЯ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Калужин Е.А.[1], Чижевский В.В.[2] Email: Kaluzhin1797@scientifictext.ru

[1]Калужин Егор Александрович – магистрант,
направление: информатика и вычислительная техника;
[2]Чижевский Вадим Валерьевич – бакалавр,
направление: информационная безопасность
кафедра информационной безопасности,
Дальневосточный федеральный университет,
г. Владивосток

Аннотация: *в статье проводится анализ процесса проектирования комплексной системы защиты информации, и, как основной этап, выделяется анализ уязвимостей. Производится классификация уязвимостей по природе возникновения. Рассматриваются формальные методики оценки уязвимостей, позволяющие с помощью математического аппарата, прогнозировать характер их поведения. В заключении устанавливается связь между угрозой и уязвимостью, приводится схема взаимодействия нарушителя информационной безопасности и владельца информационных активов.*
Ключевые слова: *анализ уязвимостей, комплексная система защиты информации, угрозы информационной безопасности.*

VULNERABILITY ANALYSIS AS A KEY STEP IN THE DESIGN OF AN INTEGRATED INFORMATION SECURITY SYSTEM

Kaluzhin E.A.[1], Chizhevskiy V.V.[2]

[1]Kaluzhin Egor Aleksandrovich – undergraduated,
PROFILE: INFORMATICS AND COMPUTER FACILITIES;
[2]Chizhevskiy Vadim Valeryevich – bachelor,
PROFILE: INFORMATION SECURITY,
DEPARTMENT OF INFORMATION SECURITY,
FAR EASTERN FEDERAL UNIVERSITY,
VLADIVOSTOK

Abstract: *the article analyzes the process of designing an integrated information security system, and, as the main stage, the vulnerability analysis is highlighted. Classification of vulnerabilities by the nature of occurrence is made. Formal methods for vulnerability assessment are considered, which allow using the mathematical apparatus to predict the nature of their behavior. In conclusion, the connection between the threat and vulnerability is established, the scheme of interaction of the infringer of information security and the owner of information assets is given.*
Keywords: *vulnerability analysis, complex information security system, information security threats.*

УДК 004.056

Комплексная система защиты информации необходима для поддержания требуемого уровня информационной безопасности и существенного снижения вероятности компрометации конфиденциальной информации [1].

В настоящее время тема проектирования комплексной системы защиты информации (КСЗИ) предприятия широко обсуждается. В статье [2] предлагается алгоритм проектирования КСЗИ для предприятия энергетического комплекса. В работе [3] авторы рассматривают факторы, влияющие на выбор оптимальных средств защиты информации, необходимых для проектирования КСЗИ.

На основе проанализированных работ можно сделать вывод, что ключевым этапом при проектировании КСЗИ и выборе средств защиты информации является анализ уязвимостей предприятия. Данная проблема является актуальной на сегодняшний день.

В работе [4] автор предлагает формальную методику оценки уязвимостей информационных активов предприятия. Она основана на вероятностном подходе и учитывает следующие факторы:

1. Потенциал возможного нарушителя. Определяется на основе экспертных оценок и имеет три вербальных интерпретации: низкий, средний, высокий.

2. Источник воздействия. Нарушитель может производить атаку из-за пределов контролируемой зоны, или непосредственно находясь на объекте.

3. Канал воздействия. Атака может производиться по сетевому, техническому или социальному каналу.

4. Объект воздействия. Объектом воздействия может быть сама конфиденциальная информация, средства её обработки или же сотрудники организации.

Предложенная в данной работе методика позволяет численно оценить опасность уязвимости и, основываясь на полученных результатах, принять соответствующие меры.

В статье [5] предлагается методика моделирования жизненного цикла уязвимости с помощью поглощающей цепи Маркова. Основная идея заключается в том, чтобы разделить жизненный цикл уязвимости на определенные стадии:

1. Зарождение;
2. Обнаружение;
3. Устранение;
4. Раскрытие;
5. Реализация.

Математический аппарат позволяет представить вероятность перехода уязвимости в различные состояние как функцию времени и принять превентивные меры для снижения вероятности реализации угроз информационной безопасности.

При анализе уязвимостей важно учитывать все возможные уязвимости, а именно:

1. Уязвимости в системно программном обеспечении – слабые стороны, ошибки, баги в операционных системах. Они устраняются с помощью обновлений (патчей), выпускаемых разработчиками.

2. Уязвимости в прикладном программном обеспечении. Для функционирования предприятия используются различное прикладное ПО: программы для автоматизации процессов, программы для бухгалтерского учета, офисные утилиты и т.д. Они являются частью информационной системы и их уязвимости могут стать причиной компрометации информации.

3. Уязвимости, связанные с неграмотной настройкой и установкой средств защиты информации. Для выявления данного типа уязвимостей необходим регулярный мониторинг и аудит системы защиты информации.

4. Сотрудники, взаимодействующие с информацией ограниченного доступа, также являются уязвимым компонентом. С ними связаны угрозы внутреннего нарушителя.

Анализ уязвимостей тесно связан с разработкой модели актуальных угроз. Критически важно разделять эти понятия. Уязвимость – слабость в компоненте информационной системы, которая позволяет злоумышленнику скомпрометировать информацию[6]. Под угрозой понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к компрометации информации. Иными словами, злоумышленник использует уязвимости для реализации угроз. В общем виде схема взаимодействия злоумышленника и владельца информации представлена на рисунке 1.

Рис. 1. Общая схема взаимодействия злоумышленника и владельца информационных ресурсов

Полный перечень угроз и уязвимостей представлен в банке данных угроз Федеральной службы по техническому и экспортному контролю Российской Федерации.

Таким образом, в статье проанализирован процесс создания комплексной защиты информации. Анализ уязвимостей определен как основной этап, влияющий на выбор программно-аппаратных средств защиты информации. Были рассмотрены формальные методики по анализу уязвимостей, а также определены различные виды уязвимостей. В заключение была установлена связь между уязвимостью и угрозой информационной безопасности. На основе проделанной работы, можно сделать вывод, что анализ уязвимостей является ключевым этапом в проектировании КСЗИ и тесно связан с анализом актуальных угроз.

Список литературы / References

1. *Гришина М.В.* Организация комплексной системы защиты информации: Учебное пособие. Гелиос АРВ, 2007. 340 с.
2. *Гросман А.* К. Алгоритм разработки и внедрения комплексной системы защиты информации на предприятии энергетического комплекса // Молодой ученый, 2016. № 13. С. 311-314.
3. *Калужин Е.А., Монастырский Д.С.* Алгоритм выбора средств информационной безопасности при проектировании системы защиты информации // ModernSciencs, 2016. № 11. С. 24-27.
4. *Гросман А.К.* Методика оценки уязвимости информационных активов предприятия // ModernSciencs, 2015. № 7.
5. *Варлатая С.К., Калужин Е.А., Монастырский Д.С.* Моделирование жизненного цикла уязвимостей информационной безопасности с помощью поглощающей цепи Маркова. // Международное научное издание «Современные прикладные и фундаментальные исследования», 2016. № 4 (23).
6. *Шаханова М.В.* Современные технологии информационной безопасности: Учебно-методический комплекс. ДВФУ, 2013. 180 с.