Прокудин Александр Михайлович

АНАЛИЗ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

В статье описывается метод анализа уязвимостей любой информационной системы, предложенный специалистами по безопасности компании Microsoft. Также представлена категоризация угроз безопасности. С помощью данной методики составляется документ, содержащий описание информационной системы, ее компонент, всех потенциальных для системы угроз и мер, необходимых для их устранения.

Адрес статьи: www.gramota.net/materials/1/2013/7/37.html

Источник

Альманах современной науки и образования

Тамбов: Грамота, 2013. № 7 (74). С. 117-119. ISSN 1993-5552.

Адрес журнала: www.gramota.net/editions/1.html

Содержание данного номера журнала: www.gramota.net/materials/1/2013/7/

Рис. 2. *Дьяконские врата из иконостаса Святой Троицы из г. Дрогобыч Львовской области*

В иконостасе Святой Троицы из г. Дрогобыча достигнуто гармоническое единство резного декора и живописи икон благодаря обращению автора к народным традициям живописи, резьбы, орнаментики. Особенностью этого иконостаса является специфическая игра ажура в композиции резьбы и иконостаса в целом. Это придает композиции иконостаса легкости в композиции и построении в целом.

Тему применения орнаментальных мотивов традиционного народного искусства в декоре иконостасов, как и церквей в целом, невозможно изложить во всех диапазонах в одной статье. В перспективе – проведение исследований о взаимосвязи цвета и резьбы, тональности покрытия поверхности иконостаса и резьбы и прочие проблемы. Исследование этих и других аспектов нашей темы можно применить на практике при создании новых иконостасов под «народный стиль». В целом тема заслуживает более широкого изучения в направлении вышеупомянутых и других аспектов.

Список литературы

1. **Всеобщая история искусств**: в 6-ти т. М.: Государственное издательство «Искусство», 1956-1966.
2. **Драган М.** Українська декоративна різьба XVI-XVIII ст. К.: Наукова думка, 1970. 202 с.
3. **Історія українського мистецтва**: в 6-ти т. К.: УРЕ, 1966-1970.
4. **Нога О.** Український стиль в церковному мистецтві Галичини кінця XIX – початку XX століть. Львів: Українські технології, 1999. 160 с.
5. **Одрехівський Р.** Сакральна різьба по дереву в Галичиніі XIX – першої половини XX століть (історія та художні особливості). Львів: Афіша, 2006. 288 с.
6. **Селівачов М.** Лексикон української орнаментики. К.: Редакція вісника «Ант», 2005.
7. **Станкевич М.** Українське художнє дерево XVI-XX ст. Львів: Інститут народознавства НАН України, 2002. 479 с.

УДК 004.056
Технические науки

В статье описывается метод анализа уязвимостей любой информационной системы, предложенный специалистами по безопасности компании Microsoft. Также представлена категоризация угроз безопасности. С помощью данной методики составляется документ, содержащий описание информационной системы, ее компонент, всех потенциальных для системы угроз и мер, необходимых для их устранения.

Ключевые слова и фразы: информационная система; угроза безопасности; уязвимость; моделирование и классификация угроз; анализ безопасности.

Прокудин Александр Михайлович
Новосибирский государственный университет
prokudin89@gmail.com

АНАЛИЗ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ©

Обеспечение защищенности информационной системы является одним из важнейших этапов ее разработки и поддержки. Очевидно, что информационная система, отданная в производство без каких-либо

средств защиты от угроз, не несет никакой практической и материальной ценности. Например, система совершения и обработки торговых сделок, реализованная без использования алгоритмов шифрования, не может гарантировать целостность обрабатываемых данных. Естественно, такая система не должна и не будет использоваться в реальных торговых операциях.

При проектировании любой новой информационной системы, а также при использовании уже реализованной системы стоит проблема гарантии ее защищенности от компрометации. Гарантия нужна не только для конечного пользователя, но и, например, для лица, выделяющего средства на разработку информационной системы. Анализ защищенности разрабатываемой системы рекомендуется проводить с помощью моделирования потенциальных угроз. В последнее время новые уязвимости появляются каждый день, поэтому важно уметь классифицировать угрозы и оценивать их по степени риска.

Информационная безопасность определяется всеми аспектами, связанными с достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки.

Защита информации должна носить комплексный характер, однако, необходимо учитывать возможность возникновения угроз, специфичных для данной информационной системы. На этапе проектирования системы защиты информации важно не упустить существенных деталей и, в то же время, не переоценить некоторые из них. Необходимо знать о характере возможных опасностей, классифицировать угрозы и проводить меры по их устранению.

Основной принцип обеспечения безопасности информационной системы лежит в анализе потенциальных угроз, проведении мер по их устранению и последующем анализе состояния безопасности системы. Моделирование угроз позволяет структурировать процесс обеспечения безопасности информационной системы и обозначить угрозы, которые способны нанести наибольший ущерб и которые необходимо устранить в первую очередь.

Нельзя обеспечить безопасность информационной системы без должного понимания специфики и происхождения угроз. Обычно, уязвимости устраняются по мере их обнаружения, часто случайным образом. Используя этот подход, невозможно ответить на вопрос: «Достаточно ли безопасна информационная система?».

Моделирование угроз не является единовременным процессом. Это итеративный подход, который начинается с ранних стадий разработки системы и продолжается на протяжении всего ее жизненного цикла. Необходимость итеративного подхода обусловлена двумя причинами. Во-первых, физически невозможно обнаружить и зафиксировать все потенциальные для системы угрозы за один раз. Во-вторых, разрабатываемое приложение (информационная система) непременно адаптируется под постоянно изменяющиеся пользовательские и функциональные требования. Поэтому моделирование угроз необходимо повторять на протяжении всего развития информационной системы.

Специалисты по безопасности компании *Microsoft* предложили процесс моделирования угроз, состоящий из шести этапов [1]:

1. Определение защищаемых ресурсов.
2. Обзор архитектуры.
3. Декомпозиция системы.
4. Определение угроз.
5. Документация угроз.
6. Приоритезация угроз.

На первом этапе определяются все ресурсы, которые необходимо защищать. Это могут быть конфиденциальные данные, базы данных, веб-страницы и т.д. Далее проводится документация функций информационной системы, ее архитектуры, физической конфигурации и технологий, использованных для ее реализации. Возможен поиск уязвимостей в дизайне информационной системы. Определение используемых в реализации технологий поможет не упустить специфичных для них уязвимостей и в дальнейшем сконцентрироваться на их устранении.

На этапе декомпозиции система разбивается на компоненты для создания профиля безопасности (который описывает реализацию аутентификации, авторизации, криптографии и других аспектов безопасности в системе). Проверяются основные вопросы безопасности, выделяются границы доверия, потоки данных и их входные точки. Система анализируется на исполнение следующих свойств: проверка пользовательских данных, аутентификация и авторизация, криптографическая защита передачи данных, управление исключениями, аудит и др. Профиль безопасности описывает реализацию аутентификации, авторизации, криптографии и других аспектов безопасности в системе.

Далее определяются потенциальные угрозы для всех компонент системы. Компания *Microsoft* предлагает методику **STRIDE** для определения и категоризации угроз [2]. Моделирование при помощи **STRIDE** поможет обеспечить исполнение в информационной системе всех свойств безопасности.

STRIDE – аббревиатура от:

- **S**poofing Identity (подмена личности).
- **T**ampering with Data (изменение данных).
- **R**epudiation (отказ от совершенной операции).
- **I**nformation Disclosure (разглашение сведений).
- **D**enial of Service (отказ в обслуживании).
- **E**levation of Privilege (повышение прав доступа).

По этой методике определяются угрозы для каждого компонента информационной системы в зависимости от категории угрозы.

Угрозы типа «Подмена личности» актуальны для систем, в которых реализуются разные уровни доступа пользователей. Пользователь не должен иметь возможность притвориться другим пользователем или прочитать атрибуты другого пользователя.

Угрозы типа «Изменение данных» реализуют возможность пользователя повлиять на логику работы системы через доступные интерфейсы. Система должна тщательно проверять все исходящие от пользователя данные в процессе их использования и вплоть до момента их сохранения в системе.

При недостаточном аудите транзакций в системе угрозы типа «Отказ от совершенной операции» реализуют возможность пользователя отказаться от выполненных им каких-либо действий в системе, что может повлиять на достоверность циркулирующей по системе информации. Например, пользователь может заявить «Я не перечислял денежные средства на этот счет». При недостаточном аудите операций невозможно проверить данное заявление.

Угрозы типа «Разглашение сведений» реализуют возможность публикации конфиденциальных данных в системе. Возможно, в системе обнаружится утечка информации.

Дизайнеры системы также должны учитывать тот факт, что на нее будут проводиться атаки типа DoS (отказ в обслуживании). Необходимо убедиться, что ресурсоемкие процессы будут недоступны неавторизованным пользователям. Такими процессами могут являться: чтение больших файлов, сложные вычисления, исполнение длинных запросов к базе данных и т.д.

Если в системе различаются пользовательские и административные роли, то необходимо убедиться в невозможности повышения прав доступа. Все действия в системе должны проверяться по матрице доступа.

На следующем этапе моделирования все определенные угрозы необходимо зафиксировать в представленном далее виде:

- Описание угрозы.
- Объект возможной атаки.
- Риск.
- Возможный сценарий атаки.
- Предпринимаемые меры по устранению угрозы.

На последнем этапе процесса расставляются приоритеты по устранению угроз в зависимости от их риска. Это позволит заняться в первую очередь угрозами, которые могут нанести системе наибольший ущерб. Экономически невыгодно устранять абсолютно все определенные угрозы, поэтому возможно опустить угрозы, вероятность реализации которых стремится к нулю и ущерб от которых минимален.

В итоге, для разработчиков информационной системы представляется документ, позволяющий им сформировать отчетливое понимание о потенциальных угрозах и рисках.

Список литературы

1. **Meier J. D., Mackman A., Dunner M., Vasireddy S., Escamilla R., Murukan A.** Improving Web Application Security: Threats and Countermeasures [Электронный ресурс]. URL: http://msdn.microsoft.com/en-us/library/ff648644.aspx (дата обращения: 10.06.2013).
2. **The STRIDE Threat Model** [Электронный ресурс]. URL: http://msdn.microsoft.com/en-us/library/ee823878%28v=cs.20%29.aspx (дата обращения: 10.06.2013).

УДК 323.1
Политология

В статье анализируются научные подходы зарубежных авторов к осмыслению феномена национализма. Внимание фокусируется на политическом аспекте данного явления. В процессе теоретического исследования установлено, что в рассматриваемых воззрениях отводится различное место политической составляющей, играющей важную роль в процессе формирования и развития национализма. Приоритет ей отдается в инструменталистском и дискурсивном подходах.

Ключевые слова и фразы: национализм; политическая составляющая национализма; примордиализм; конструктивизм; инструментализм; дискурсивный подход.

Пустошинская Ольга Сергеевна, к. полит. н.
Доронин Евгений Дмитриевич
Тюменский государственный университет
pustoshinskayaolga@yandex.ru; doroninzenia@rambler.ru

ПОЛИТИЧЕСКИЙ АСПЕКТ НАЦИОНАЛИЗМА: АНАЛИЗ ЗАРУБЕЖНЫХ ПОДХОДОВ©

Несмотря на то, что в зарубежной науке создана обширная теоретико-методологическая база исследований национализма, неоднозначность восприятия общественным сознанием сущности данного явления обуславлива-