Чернова Екатерина Владимировна
студентка
Молчанова Наталия Николаевна
студентка
Молчанова Надежда Николаевна
студентка
ФГБОУ ВО «Оренбургский государственный университет»
г. Оренбург, Оренбургская область

БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Аннотация*: в данной статье авторами рассматривается вопрос основных требований к безопасности программного обеспечения, политике безопасности и механизмам, которые обеспечивают соблюдение этой безопасности.*

Ключевые слова*: политика безопасности, аутентификация, авторизация, аудит, конфиденциальность, целостность, доступность.*

При рассмотрении общих требований для программного обеспечения, которое хотим создать, мы должны также учитывать его требования к безопасности. Требования безопасности обрисовывают ожидания защиты работы ПО, и эти требования бывают двух видов. Во-первых, существует цели и политики, связанные с безопасностью. Во-вторых, чтобы соблюдать безопасность, мы должны иметь требования к механизмам, которые мы используем. Например, можно потребовать, чтобы для аутентификации на основе пароля, пароли были сильными (не менее 8 символов). База данных с паролями не должна быть доступна для любой программы, кроме программы аутентификации логина.

Теперь давайте копнём немного глубже и изучим различные виды политик и механизмы, которые проектировщик может использовать. Существует три классических типа политик безопасности – политика конфиденциальности, целостности и доступности. Политика конфиденциальности иногда подразделяется на неприкосновенность частной жизни и требования анонимности. Обязатель-

ные механизмы защиты часто затрагивают три вида деятельности – аутентификация, авторизация и проведение аудита. Давайте рассмотрим каждый из этих элементов более подробно.

Во-первых, мы будем учитывать три вида политик безопасности, начиная с неприкосновенности частной жизни и конфиденциальности. Секретность и конфиденциальность обеспечиваются, если эта важная информация является не доступной для неавторизированных пользователей. Мы, как правило, относим к этому свойства, такие как неприкосновенность частной жизни для физического лица, а также конфиденциальность данных. Нарушение неприкосновенности частной жизни или конфиденциальности может произойти непосредственно, или может произойти с побочной стороны. Другой тип конфиденциальности политика анонимности. Это особый вид конфиденциальности.

Следующий вид политики безопасности, который мы будем рассматривать, это политика целостности. Идея заключается в том, что чувствительная информация не должна быть повреждена при действиях неавторизированных пользователей. Например, только владелец счета может разрешить снятие средств со своего счета. Если какая-либо другая сторона смогла повлиять на счёт вывода, то это нарушило бы целостность баланса банковского счета. Таким образом, нарушение целостности может быть прямым или косвенным. Например, у нас есть возможность специально снимать деньги со счета, потому что система неправильно разрешает совершать подобные действия. Или, мы можем вводить систему в заблуждение, чтобы достичь своих целей.

Третий вид политики безопасности – это доступность. В этом случае, доступность означает, что система реагирует на запросы, которые приходят к ней. Например, мы можем захотеть, чтобы пользователь всегда имел доступ к своему счеты для каких-либо запросов или снятие денег со счёта.

После того, как мы определили политику безопасности для приложения, мы должны думать о том, каким образом будем обеспечивать соблюдение этой безопасности. Лесли Лэмпорт определил золотой стандарт (gold standart), который

состоит из трёх механизмов – аутентификации, авторизации и аудита. Рассмотрим первый элемент золотого стандарта – аутентификацию. Цель аутентификации – определить, какими правами будет обладать текущий субъект. В частности, многие политики безопасности требуют понятия идентичности. Для того чтобы разрешить то или иное действие, мы должны знать, кто именно его хочет выполнить (какими правами он обладает). То есть мы должны определить, кто субъект, и будет ли его действие разрешено в соответствии с нашей политикой безопасности.

Следующим элементом золотого стандарта является авторизация. Авторизация определяет, когда принципал может выполнить определённое действие. Например, Ване разрешён доступ к своему собственному счёту, но он не имеет права доступа к счёту Алисы. Существуют самые разнообразные политики безопасности, которые включают некоторые виды авторизаций.

Завершающим элементом золотого стандарта является аудит. Здесь идея состоит в том, чтобы удержать достаточно информации, чтобы иметь возможность определить обстоятельства нарушений, или установить, что эти нарушения не происходят. Такая информация часто хранится в лог-файлах – файлах с записями о событиях в хронологическом порядке. То есть мы должны защитить эти файлы от несанкционированного доступа.

В заключении хочется отметить, что осуществлять требования безопасности нужно в соответствии с целями вашей организации. Вы должны оценить все слабые места в системе, осуществить моделирование потенциальных угроз. Таким образом, вы определяете ресурсы, которые должны защищать. И в дальнейшем определить политику безопасности и механизмы, которые будут направлены на срыв потенциальных угроз.

Список литературы

1. Introduction to Computer Security [Электронный ресурс]. – Режим доступа: http://its.ucsc.edu/security/training/intro.html

2. Computer Security [Электронный ресурс]. – Режим доступа: http://www.consumer.ftc.gov/articles/0009-computer-security

3. Введение в информацию безопасности [Электронный ресурс]. – Режим доступа: http://www.kolomna-school7-ict.narod.ru/st30301.htm