УДК 004.451 **Информационные технологии**

Кулавская Юлия Евгеньевна, *студентка факультета довузовской подготовки и среднего профессионального образования,*
ФГБОУ ВО «Мордовский государственный университет им. Н.П. Огарёва»

ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: В данной статье рассматриваются основные принципы обеспечения информационной безопасности. Также приводятся примеры из жизни для понимания сути.

Ключевые слова: информационная безопасность, система, информация, конфиденциальность.

Annotation: This article discusses the basic principles of information security. There are also examples from life for understanding the essence.

Keywords: information security, system, information, confidentiality.

В широком понимании информационную безопасность можно охарактеризовать как совокупность средств защиты информации от воздействия, будь то случайное или умышленное. Владельцу информации наносится ущерб вне зависимости от того, какими факторами было вызвано воздействие (естественными или искусственными).

Команда специалистов может обеспечить наивысшую степень безопасности системы, лишь используя основные принципы информационной безопасности.

Принципы информационной безопасности

Вся система обеспечения информационной строится на шести основных принципах:

– наименьшей привилегии;
– разделения обязанностей;
– глубокой защиты;
– безопасного отказа;
– открытого проектирования;
– минимизации площади поверхности атаки.

1. Принцип наименьшей привилегии [3].

Принцип наименьших привилегий означает, что можно гарантировать людям доступ только к тому, что им нужно для выполнения своей работы. Например, если разработать систему, которая содержит конфиденциальную финансовую информацию о клиентах, рекомендуется ограничить доступ к этой информации. Человек, который отвечает на телефонные звонки и назначает встречи, вероятно, не нуждается в доступе ко всей конфиденциальной информации. С другой стороны, менеджер по работе с клиентами, вероятно, нуждается в доступе к этой информации. Главное — убедиться, что менеджер по работе с клиентами не имеет доступа к информации из учетных записей, которыми он не управляет.

Гарантируя, что учетные записи имеют только привилегии, необходимые для выполнения своей работы, можно утверждать, что если злоумышленник компрометирует учетную запись, то он получит минимальное количество информации. Это уменьшает потери от атаки.

2. Принцип разделения обязанностей [3].

Принцип разделения обязанностей вытекает из принципа наименьшей привилегии. Идея разделения обязанностей заключается в том, что ни одна отдельная роль не должна иметь слишком большого авторитета. Это отличается от концепции наименьших привилегий. В то время как это фокусируется на том, чтобы люди имели только те привилегии, которые им нужны для выполнения своей работы, это означает, что их работа не слишком велика. Когда кто-то делает слишком большую работу, ему понадобится много разрешений для выполнения этой работы. Кроме того, когда у кого-то много

обязанностей на работе, это означает, что он подвержен принятию неправильных решений.

Проще говоря, есть система и её владельцы не желают, чтобы человек, ответственный за продажи, также мог утверждать скидки. У этого человека будет стимул изменить программное обеспечение, и он может принимать неверные решения о скидках, чтобы увеличить свои продажи. Вместо этого кто-то другой, например, менеджер, должен одобрить скидку до окончания продажи.

3. Принцип глубокой защиты [4].

Принцип глубокой защиты немного отличается от предыдущих принципов. В то время как наименьшие привилегии и разделение обязанностей контролируют процесс получения людьми доступ к системе, глубокая защита — предотвращает доступ к системе. Основной идеей данного принципа является то, любая система безопасности потерпит неудачу. Обойти компьютерные системы безопасности может быть очень трудно, но это всегда возможно.

Проектирование с глубокой защитой означает создание систем, которые сообщат, когда назначенная безопасность потерпит неудачу. Например, многие серверы для программных систем используют программное обеспечение безопасности, но расположены в одном здании. Кто-то имел физический доступ к каждому из серверов. Внезапно этот причудливый брандмауэр или программное обеспечение для обнаружения вторжений становятся бесполезными. Вот почему центры обработки данных спроектированы с присутствием физической безопасности и камерами безопасности для обнаружения злоумышленников.

4. Принцип безопасного отказа.

Как и в случае с глубокой защитой, этот принцип распознает, что все идет к провалу. Чтобы предусмотреть, как система может выйти из строя с наименьшими потерями.

Объяснить смысл данного принципа можно на примере офисного здания. У злоумышленника каким-то образом оказались ключи от всех дверей в здании и ему не составит труда получит то, зачем он пришёл. В системе, которая предусматривает подобную ситуацию и надежно выходит из строя, все двери запираются. Вместо того, чтобы предоставить доступ ко всем дверям в здании, у злоумышленника не окажется доступа ни к одной из них.

Та же концепция применима и к разработке программного обеспечения. Система, предназначенная для безопасного отказа, предоставляет доступ к частям системы только тогда, когда каждый шаг процесса завершается успешно.

5. Принцип открытого проектирования [2].

Принцип открытого проектирования гласит, что безопасность системы не должна зависеть от секретности реализации. Это особенно важный принцип для таких концепций безопасности, как криптографические реализации. Хорошо разработанные криптографические реализации публикуются публично. Их тестируют самые умные люди в мире, прежде чем применить на практике.

6. Принцип минимизации площади поверхности атаки.

Принцип минимизации площади поверхности атаки заключается в удалении частей системы/приложения, чтобы сделать его более безопасным.

Для более простого понимания можно снова привести в пример офисное здание. Как и у любого сооружения, у офисного здания есть стены, двери, окна. Можно поставить на двери самые современные замки и системы защиты, но чем больше в здании окон, тем больше вероятность, что через одно из них может забраться злоумышленник. Ведь окна в свою очередь не так сильно подвергаются защите.

Части системы подобны окнам. Они выглядят красиво, но могут раскрыть функциональность, которая приведет к ошибкам. Минимизация площади поверхности атаки ставит вопрос о том, является ли функция необходимой. Иногда, перепроектируя функцию, чтобы сделать ее более простой, общая безопасность приложения улучшается.

Информационная безопасность — это сложная работа, требующая внимания к деталям и более высокого уровня осведомленности одновременно. Как и многие сложные задачи, если разбить их на основные этапы, процесс можно упростить.

Библиографический список:

1. Андреева Н.А. и др. Основные принципы и методы разработки правил политики информационной безопасности //Современные технологии обеспечения гражданской обороны и ликвидации последствий чрезвычайных ситуаций – 2014. – №1(5).

2. Гусев М.О. Открытые информационные системы и защита информации //Журнал радиоэлектроники – 2005. – №3.

3. Основы информационной безопасности URL: https://intuit.ru/studies/courses/10/10/lecture/324.

4. Программно-аппаратная защита информации URL: http://www.chemisk.narod.ru/html/ib04.html.

5. Шибарова Е. В. и Винокурова О. А. Безопасность промышленных информационных систем, виды угроз и общие принципы защиты информации // Вестник Московского государственного университета печати – 2016. – № 26.