ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ

Ибадуллаева Зарнигор
Политехнический техникум № 1 Хазораспского района
Учитель «Информатика и ИТ»

INFORMATION SECURITY: THREATS AND METHODS OF PROTECTION

Аннотация. В этой статье полностью раскрыта тема по информационной и системной безопасности, рассматривается понятие информационной безопасности и о её угрозах, об- щий смысл, методы и способы защиты информации.

Abstract. This article fully covers the topic of information and system security, discusses the concept of information security and its threats, the general meaning, methods and ways to protect information.

Ключевые слова: информационная безопасность, угрозы, вирусы, черви, фишинговые атаки, троянские кони, методы защиты.

Keywords: information security, threats, viruses, worms, phishing attacks, trojan horses, pro- tection methods.

Информационная безопасность — состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере, все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостно- сти, доступности, неотказуемости, подотчётности, аутентичности и достоверности информа- ции или средств её обработки.

Безопасность информации определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамерен- ными воздействиями на данные и (или) на другие ресурсы, используемые в автоматизиро- ванной системе.

Чтобы стандартизировать эту дисциплину, ученые и специалисты сотрудничают и стремятся установить базовые рекомендации, политики и отраслевые стандарты в отноше- нии паролей, антивирусного программного обеспечения, брандмауэра, программного обес- печения для шифрования, юридической ответственности и стандартов обучения пользовате- лей/администраторов. Эта стандартизация может в дальнейшем основываться на разнообразных законах и нормативных актах, которые влияют на доступ, обработку, хране- ние и передачу данных. Однако реализация любых

стандартов и руководств внутри органи- зации может иметь ограниченный эффект, если не принимать культуру постоянного улучше- ния.[1]

Угрозы информационной безопасности бывают разных форм, одними из наиболее рас- пространенных сегодня угроз являются программные атаки, кража интеллектуальной соб- ственности, кража личных данных, кража оборудования или информации, саботаж и вымога- тельство информации. Большинство людей испытали какие-то программные атаки. Вирусы, черви фишинговые атаки и троянские кони- вот несколько распространенных примеров про- граммных атак. По аспекту информационной безопасности, на который направлены угрозы:

- Угрозы конфиденциальности(неправомерный доступ к информации). Угроза наруше- ния конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Она имеет место, когда получен доступ к некоторой информации ограниченного доступа, хранящейся в вычислительной системе или передаваемой от одной системы к другой
- Угрозы целостности(неправомерное изменение данных). Угрозы нарушения целост- ности – это угрозы, связанные с вероятностью модификации той или иной информации, хра- нящейся в информационной системе. Нарушение целостности может быть вызвано различ- ными факторами – от умышленных действий персонала до выхода из строя оборудования.
- Угрозы доступности(осуществление действий, делающих невозможным или затруд- няющих доступ к ресурсам информационной системы). Нарушение доступности представля- ет собой создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных биз- нес-целей.

Правительства, военные, корпорации, финансовые учреждения, больницы и частные предприятия накапливают много конфиденциальной информации о своих сотрудниках, кли- ентах, продуктах, исследованиях и финансовом положении. Если конфиденциальная инфор- мация о клиентах, финансах или новой линейке продуктов попадет в руки конкурента или хакера, то бизнес и его клиенты могут понести повсеместные, непоправимые финансовые потери, а также нанести ущерб репутации компании. С точки зрения бизнеса информацион- ная безопасность должна быть сбалансирована с затратами; модель Гордон-Loeb обеспечива- ет математически-экономический подход для решения этой проблемы.[2]

Для человека информационная безопасность оказывает существенное влияние на кон- фиденциальность, которая рассматривается в разных культурах по-разному. Возможные от- веты на угрозу безопасности или риск:

- уменьшить/смягчить-внедрить меры защиты и контрмеры для устранения уязвимо- стей или блокирования угроз
- назначить/передать-разместить стоимость угрозы для другой организации или органи- зации, например, для покупки страховки или аутсорсинга
- принять-оценить, перевешивает ли стоимость контрмер возможную стоимость потери из-за угрозы.[3]

Методы и способы защиты информации содержат в себе конкретные меры и техноло- гии к решению проблем по информационной безопасности предприятия. На текущий момент методы защиты можно разделить на несколько основных групп. Итак, классификация мето- дов и способов защиты выглядит следующим образом: способы изменение вида и структуры передачи информации в сети и ее хранения, например применение криптографических мето- дов защиты; организационные методы защиты данных, основанные на управлении информа- ционными системами и регламентирование правил безопасности; технические и технологи- ческие методы защиты информации, подразумевающие использования специальных программных и аппаратных средств. Комплексная защита информации создается на объектах для блокирования (парирования) всех возможных или наиболее вероятных угроз безопасно- сти информации. Для парирования той или иной угрозы используется определенная сово- купность средств и методов защиты, некоторые из них защищают от нескольких угроз одно- временно.

Среди методов защиты имеются и универсальные методы, являющиеся базовыми при построении любой системы защиты.

Правовые методы защиты информации служат основой легитимного построения и ис- пользования системы защиты любого назначения

Организационные методы защиты информации используются для парирования не- скольких угроз, кроме того, их использование в любой системе защиты обязательно.[4]

На крупных предприятиях методами, защищающими информационную безопасность, должна заведовать специальная служба безопасности компании. Ее сотрудники должны искать способы воздействия на информацию и устранять всевозможные прорывы злоумыш- ленников. По локальным актам разрабатывается политика безопасности, которую важно строго соблюдать. Стоит обратить внимание и на исключение человеческого фактора, а так- же поддерживать в исправности все технические средства, связанные с безопасностью ин- формации. Задержки у атакующей информационную безопасность стороны возможны толь- ко в связи с прохождением системы защиты. Абсолютных способов обезопасить себя от угроз не существует,

поэтому информационную систему защиты требуется всегда усовер- шенствовать, поскольку мошенники тоже усовершенствуют свои методики. Пока не приду- ман универсальный способ, который подходит каждому и дает стопроцентную защиту. Важ- но остановить проникновение злоумышленников на раннем уровне.

Список литературы:

1. Счлиенгер, Томас, Теуфель, Стефани «Культура информационной безопасности - от ана- лиза к изменениям». SAICSIT:. 2003
2. Гордон, Лоуренс, Леб, Мартин «Экономика информационной безопасности инвестиций». ACM ТИСС 2002. с. 438–457.
3. Стюарт, Джеймс.CISSP Сертифицированное профессиональное учебное пособие по без- опасности информационных систем. Канада: 2012 с. 255–257.
4. А.А.Безбогов, А.В.Яковлев, В.Н.Шамкин «Методы и средства защиты компьютерной информации». ТГТУ: