УДК 00 – 37.02

Сапбыева Айгуль
преподаватель кафедры информационных систем
Института Телекоммуникаций и информатики
Туркменистана,
Атаев Мекан
студент третьего курса
Института Телекоммуникаций и информатики
Туркменистана,
Ашхабад, Туркменистан.

ОСНОВНЫЕ ПОНЯТИЯ ВВЕДЕНИЯ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Аннотация: В данной статье говорится об информационной безопасности, о новых проблемах этого аспекта. Даются начальные понятия, связанные с этой сферой.

Ключевые слова: Интернет, конфиденциальность, целостность, доступность, аутентификация, авторизация.

Sapbyeva Aigul
lecturer of the Department of Information Systems
Institute of Telecommunications and Informatics
Turkmenistan,
Ataev Mekan
third year student
Institute of Telecommunications and Informatics
Turkmenistan
Ashgabat, Turkmenistan.

BASIC CONCEPTS INTRODUCTION TO INFORMATION SECURITY

Annotation: This article talks about information security, about new problems in this aspect. The initial concepts related to this sphere are given.

Key words: Internet, confidentiality, integrity, availability, authentication, authorization.

Интернет — это не единая сеть, а всемирное собрание слабо связанных сетей, которые доступны с отдельных компьютерных хостов различными способами любому, у кого есть компьютер и подключение к сети. Таким образом, отдельные лица и организации могут получить доступ к любой точке Интернета независимо от национальных или географических границ или времени суток. Однако наряду с удобством и

легким доступом к информации возникают риски. Среди них риски того, что ценная информация будет потеряна, украдена, изменена или использована не по назначению. Если информация записана в электронном виде и доступна на сетевых компьютерах, она более уязвима, чем, если бы та же информация была напечатана на бумаге и заперта в картотеке. Злоумышленникам не нужно входить в офис; они могут быть даже не в одной стране. Они могут украсть или подделать информацию, не прикасаясь к листу бумаги или копировальному аппарату. Они также могут создавать новые электронные файлы, запускать собственные программы и скрывать доказательства своей несанкционированной деятельности.

Основные концепции безопасности. Три основные концепции безопасности, важные для информации в Интернете, — это **конфиденциальность, целостность и доступность.** Концепции, относящиеся к людям, которые используют эту информацию, включают **аутентификацию, авторизацию.**

Когда информация читается или копируется кем-то, кто не уполномочен на это, результатом является потеря конфиденциальности. Для некоторых видов информации конфиденциальность является очень важным атрибутом. Примеры включают данные исследований, медицинские и страховые записи, спецификации новых продуктов и корпоративные инвестиционные стратегии. В некоторых местах может существовать юридическое обязательство по защите частной жизни людей. Это особенно верно для банков и кредитных компаний; сборщики долгов; предприятия, которые предоставляют кредит своим клиентам или выпускают кредитные карты; больницы, кабинеты врачей и медицинские испытательные лаборатории; лица или агентства, которые предлагают такие услуги, как психологическое консультирование или медикаментозное лечение; и агентства, которые собирают налоги.

Информация может быть повреждена, когда она доступна в небезопасной сети. Когда информация изменяется неожиданным образом, результат известен как потеря целостности. Это означает, что в информацию вносятся несанкционированные изменения, будь то человеческая ошибка или умышленное вмешательство. Целостность особенно важна для важных данных о безопасности и финансовых данных, используемых для таких операций, как электронные денежные переводы, управление воздушным движением и финансовый учет.

Информация может быть стерта или стать недоступной, что приведет к потере доступности. Это означает, что люди, уполномоченные на

получение информации, не могут получить то, что им нужно. Доступность часто является самым важным атрибутом в сервисно-ориентированном бизнесе, который зависит от информации (например, расписания авиакомпаний и системы онлайн-инвентаризации).

Чтобы сделать информацию доступной для тех, кто в ней нуждается и кому можно ее доверить, организации используют *аутентификацию и авторизацию.* Аутентификация подтверждает, что пользователь является тем человеком, за которого себя выдает. Это доказательство может включать что-то, что знает пользователь (например, пароль), что-то, что есть у пользователя (например, «смарт-карта»), или что-то о пользователе, который подтверждает личность человека (например, отпечаток пальца). Авторизация — это действие по определению того, имеет ли конкретный пользователь (или компьютерная система) право выполнять определенные действия, такие как чтение файла или запуск программы.

Аутентификация и авторизация идут рука об руку. Пользователи должны быть аутентифицированы перед выполнением действий, на выполнение которых они уполномочены. Безопасность надежна, когда средства аутентификации не могут быть впоследствии опровергнуты — пользователь не может позже отрицать, что он или она выполнили действие.

Эти концепции информационной безопасности также применимы к термину *информационная безопасность*; то есть пользователи Интернета хотят быть уверены, что

• они могут доверять информации, которую используют;

• информация, за которую они несут ответственность, будет передаваться только в том порядке, в котором они ожидают;

• информация будет доступна, когда они в ней нуждаются;

• системы, которые они используют, будут обрабатывать информацию своевременно и надежно;

Кроме того, информационная гарантия распространяется на системы всех типов, включая крупномасштабные распределенные системы, системы управления и встроенные системы, и охватывает системы с аппаратными, программными и человеческими компонентами.

Безобидная на первый взгляд информация может подвергнуть компьютерную систему компрометации. Информация, которую злоумышленники сочтут полезной, включает в себя используемое аппаратное и программное обеспечение, конфигурацию системы, тип сетевых подключений, номера телефонов, а также процедуры доступа и аутентификации. Информация, связанная с безопасностью, может

позволить неавторизованным лицам получить доступ к важным файлам и программам, что ставит под угрозу безопасность системы. Примерами важной информации являются пароли, файлы и ключи управления доступом, информация о персонале и алгоритмы шифрования.

На современном этапе развития аспекта информационной безопасности разрабатываются новые проекты при усовершенствовании всех элементов безопасности в сети. И это дает возможность использовать информацию в электронном формате несмотря на некоторые сложности при сохранении.

Литература:

1. Андриоле, С. (2014). Готовая технология: быстрое отслеживание новых бизнес-технологий. Связь АКМ, 57(2), 40–42.

2. Бодин, Л., Гордон, Л.А., и Леб, М.П. (2008). Информационная безопасность и управление рисками. Сообщения ACM, 51 (4), 64–68.

3. Зафар, Х. (2011). Управление рисками безопасности в фирме из списка Fortune 500: тематическое исследование. Журнал информационной конфиденциальности и безопасности, 7 (4), 23–53.