Свойства компьютерной информации, важные с точки зрения информационной безопасности: конфиденциальность, целостность и доступность.

Реферат по индивидуальному докладу

Манаева Варвара Евгеньевна

Содержание

1 Компьютерная информация – что это? 5

2 Свойства компьютерной информации 7

2.1 Конфиденциальность 8

2.2 Целостность 9

2.3 Доступность 11

3 Заключение 13

4 Список литературы 14

Список иллюстраций

Список таблиц

1 Компьютерная информация – что это?

Современный уровень развития научного знания еще не позволяет, а возможно и никогда не позволит, дать точное и законченное определение понятия «информация». С развитием нашего представления о мире, с развитием науки содержание этого понятия расширяется и углубляется.

Норберт Винер в своей работе «Кибернетика или управление и связь в животном и машине» определяет информацию как «обозначение содержания, черпаемого нами из внешнего мира в процессе приспособления к нему и приведения в соответствие с ним нашего мышления». Т.е. информация определяется через категорию «содержание внешнего мира» и напрямую увязана с человеком, его мышлением и процессом приспособления человека к явлениям и событиям внешнего мира. Иными словами, Винер утверждает, что информация вне человеческого сознания не существует.

Отождествление информации со сведениями или фактами, которые теоретически могут быть получены и усвоены, то есть, преобразованы в человеческие знания, составляет суть антропоцентрического подхода к определению понятия «информация».

До последнего времени антропоцентрический подход удовлетворительно работал в области правовых и общественных наук. Однако в связи с широким внедрением вычислительной техники его недостатки все чаще дают о себе знать. Во-первых, подход к информации только как к сведениям не позволяет адекватно

интерпретировать информационные процессы в таких объектах, как компьютерные программы, компьютерные сети, системы искусственного интеллекта, системы, ориентирующиеся в состоянии неопределенности. Здесь процессы получения, преобразования, передачи информации могут проходить без этапа осмысления их человеком. Во-вторых, в рамках антропоцентрического подхода невозможно найти адекватного объяснения генетической информации живой природы. В связи с этим возникла потребность в изменении трактовки понятия информации. Оно было расширено и включило обмен сведениями не только между человеком и человеком, но также «между человеком и автоматом, автоматом и автоматом, обмен сигналами в животном и растительном мире, передачу признаков от клетки к клетке».

Наиболее плодотворное проникновение в сущность понятия «информация» осуществил К. Шеннон в работах, опубликованных в конце 40-х годов XX в. В них под информацией понимаются лишь те сообщения, которые уменьшают неопределенность у получателя этого сообщения. Таким образом, по Шеннону информация – величина, обратная энтропии, то есть неопределенности.

Согласно действующему ФЗ «Об информации, информационных технологиях и защите информации» [1], определение конфиденциальности выглядит как:

“Информация – сведения (сообщения, данные) независимо от формы их представления”

2 Свойства компьютерной информации

Хотя формального определения информации не существуют, среди исследователей не возникает споров относительно её свойств. В многочисленных трудах по кибернетике, информационным технологиям, а также в юридических учебниках содержание понятия «информация» зачастую раскрывается через её свойства. Число этих свойств у разных исследователей неодинаково, но связано это лишь с тем, что в рамках отдельной научной дисциплины не все свойства информации имеют значение.

Так, например, изучая информацию как особый объект судебной экспертизы и сравнивая свойства материальных и информационных объектов, С.А. Смирнова подробно описывает 21 различие. В учебнике «Правовая информатика» Чубуковой С.Г. И Элькина В.Д. таких значимых с точки зрения авторов свойств девять, в том числе неисчерпаемость, массовость, универсальность и т.д. Причем, говоря о свойстве «качество», авторы разлагают его на восемь других свойств, таких как полнота, избыточность, адекватность, актуальность и т.д.

Для компьютерной информации выделяют три центральных свойства, изучаемых в рамках информационной безопасности:

- конфиденциальность,
- целостность
- и доступность.

Их принципиальное отличие от всех остальных свойств заключается в том,

что они не присущи информации как таковой, а появляются лишь в результате принятия мер иного, организационного характера. Более того, после того как определенная информация (или компьютерная информация) обрела эти свойства, она может их и лишиться – в результате внешних воздействий. Эти воздействия могут явиться как результатом события (например, в результате стихийного бедствия был уничтожен банк данных – потеря целостности и доступности), так и действия. В свою очередь, действия могут быть правомерные и неправомерные. Учитывая, что информация, обладающая указанными свойствами (всеми тремя или двумя последними) имеет гораздо большую ценность, чем информация, такими свойствами не обладающая, наиболее тщательно при организации систем хранения информации нужно следить именно за состоянием конфиденциональности, целостности и доступности информации.

2.1 Конфиденциальность

Если информация обладает свойством конфиденциальности, то доступ к этой информации должен иметь ограниченный круг лиц или организаций. Конфиденциальность информации нарушается при получении доступа к ней третьими лицами. Такой доступ называется несанкционированным. При этом, несанкционированный доступ к информации может быть направлен как на просто получение этой информации, так и на изменение или уничтожение информации. Согласно действующему ФЗ «Об информации, информационных технологиях и защите информации» [1], определение конфиденциальности выглядит как:

«Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя.»

Обеспечение конфиденциальности информации – один из важнейших принципов информационной безопасности. Конфиденциальность информации может быть обеспечена с помощью шифрования данных, эффективного управления

доступом, строгой идентификации пользователей, а также с помощью мониторинга сетевой активности. При грамотном построении информационной системы, обеспечение конфиденциальности способствует сохранению коммерческих секретов, личных данных и других важных и чувствительных сведений.

Особенно важное значение обеспечение конфиденциальности информации играет в отношении защиты персональных данных. Множество организаций запрашивают персональные данные людей и обязуются нести ответственность за их сбор, хранение, обработку и уничтожение из собственных хранилищ.

Конфиденциальность данных, в основном, строится на принципе доверия. Пользователи открывают доступ организациям к своим персональным данным и ожидают, что их данные будут храниться с осторожностью и не будут передаваться в руки третьих лиц, дополнительно подписывая определённый договор о личных данных (как правило, называемый офертой). При нарушении договора, пользователи могут не только перестать пользоваться услугами организации, но и повлечь для организации серьёзные юридические последствия.

На нарушении обеспечения конфиденциальности строится и **социальная инженерия** и фишинговые атаки. При таком виде мошенничества пользователя стремятся обмануть для получения доступа к конфиденциальной информации.

При обеспечении конфиденциальности информации важно поддерживать баланс между конфиденциальностью и доступностью для пользователей информации.

2.2 Целостность

Информация, обладающая свойством целостности, не изменена и не утеряна без осознанных действий создателя или обладателя информации. Согласно рекомендациям по стандартизации Р 50.1.053-2005 “Информационные технологии. Основные термины и определения в области технической защиты информации” [2], определение целостности выглядит как:

“Целостность информации (ресурсов автоматизированной информационной системы) — состояние информации (ресурсов автоматизированной информационной системы), при котором её (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право.”

Принцип целостности представляет собой неотъемлемую часть фундаментальных принципов информационной безопасности, направленных на обеспечение неприкосновенности данных. В современных условиях активного обмена информацией, где данные пересылаются, хранятся и обрабатываются в различных средах, обеспечение их неприкосновенности становится стратегически важным компонентом.

Основные аспекты гарантии целостности включают использование криптографических хэш-функций. Эти функции генерируют фиксированный размер данных, называемый хэшем, который выступает в качестве “отпечатка пальца” для контролируемых данных. Если данные подверглись хотя бы малейшему изменению, хэш изменится, что сразу сигнализирует о возможном нарушении целостности. Кроме того, контрольные суммы, являющиеся схожими инструментами, также используются для подтверждения неповрежденности данных в различных точках их жизненного цикла.

Гарантия целостности охватывает все этапы обработки данных. В процессе передачи по сети, хранения на серверах или обработки на рабочих станциях, системы должны быть настроены так, чтобы предотвратить случайные ошибки или преднамеренные модификации. При этом ключевыми элементами становятся не только технические средства, но и строгие политики управления доступом и мониторинга, направленные на поддержание целостности данных.

Целостность данных оказывает существенное воздействие на корректность и достоверность информации. Если данные подвергнуты вмешательству, это может привести к сбоям в работе системы, неверным выводам и, что более серьезно, искажению фактов, что может быть особенно критичным в сферах, где точность информации имеет решающее значение.

Принцип целостности несет в себе также важное нравственное измерение. Обеспечение целостности данных подразумевает ответственность за точность и правдивость информации. Организации и специалисты по информационной безопасности должны стремиться к созданию среды, где данные остаются неприкосновенными, и где доверие пользователей к информационным системам поддерживается честностью и надежностью обработки данных.

2.3 Доступность

Принцип доступности фокусируется на обеспечении непрерывного доступа к информационным ресурсам. В мире, где бизнес-процессы, коммуникации и услуги в значительной степени зависят от информационных технологий, обеспечение доступности становится критическим элементом стратегии информационной безопасности.

ГОСТ Р 52292-2004 Национальный стандарт РФ «Информационная технология. Электронный обмен информацией. Термины и определения» [3] определяет доступность как:

“Доступность (документа) — свойство документа, состоящее в том, что форма представления документа обеспечивает физическую возможность измерения заданных параметров этого представления документа (содержания, атрибутов, технологии) заданными средствами в заданных точках за конечное время.”

Поддержание высокой доступности требует разносторонних подходов. Это включает в себя резервирование, отказоустойчивость и тщательное планирование бизнес-процессов. Резервирование и резервные копии обеспечивают возможность быстрого восстановления после сбоев или атак, гарантируя, что важные бизнес-процессы не прерываются.

Обеспечение доступности в условиях возможных кибератак требует постоянного мониторинга, анализа и улучшения средств защиты. DDoS-атаки, направленные на перегрузку сети или серверов, представляют серьезную угрозу для

доступности. Меры для обнаружения и предотвращения таких атак становятся неотъемлемой частью стратегии.

Признание важности доступности распространяется на различные сферы деятельности. В медицинской отрасли, например, доступность к электронным медицинским записям может быть вопросом жизни и смерти. В финансовой сфере — доступность к банковским системам является ключевым параметром для предотвращения финансовых кризисов.

Принцип доступности может противостоять различным видам атак, включая физические. Пожары, наводнения, стихийные бедствия – все эти факторы могут создать ситуацию, при которой доступ к физическим или электронным ресурсам становится проблематичным. Безопасность данных включает не только кибераспекты, но и обеспечение сохранности информации в любых условиях.

Один из вызовов в обеспечении доступности – уже упомянутый баланс между открытым доступом и конфиденциальностью. Слишком строгие меры обеспечения конфиденциальности могут создавать препятствия для пользователя, в то время как отсутствие должного контроля может открыть двери для потенциальных угроз. Поэтому поиск оптимального баланса становится важной задачей для организаций.

3 Заключение

В контексте управления рисками принципы информационной безопасности выступают в роли фундаментального строительного материала. Конфиденциальность направлена на предотвращение несанкционированного доступа, целостность — на гарантирование неприкосновенности данных, а доступность — на обеспечение бесперебойного функционирования. Этот баланс позволяет организациям эффективно справляться с современными киберугрозами и предоставлять высокий уровень услуг.

Организации, стремящиеся к совершенствованию своих практик информационной безопасности, должны принимать во внимание не только технологические аспекты, но и человеческий фактор. Обучение сотрудников, разработка четких политик безопасности и регулярные аудиты являются неотъемлемыми элементами успешной стратегии.

В завершение, понимание, как принципы конфиденциальности, целостности и доступности взаимодействуют, позволяет создать устойчивую, гибкую систему безопасности, способную адаптироваться к постоянно меняющейся киберугрозовой среде. Непрерывное соблюдение этих принципов становится залогом успешного противостояния современным угрозам и создания долгосрочной устойчивости информационных систем.

Запись доклада: Ссылка на видео, Rutube

4 Список литературы

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ ”Об информации, информационных технологиях и о защите информации”. 2006.
2. Рекомендации по стандартизации Р 50.1.053-2005 ”Информационные технологии. Основные термины и определения в области технической защиты информации”. 2005.
3. Национальный стандарт РФ «Информационная технология. Электронный обмен информацией. Термины и определения» (ГОСТ Р 52292-2004). 2004. 24 с.