Тема 10.Информационная безопасность и конфиденциальность

Угрозы информационной безопасности. Вредоносное программное обеспечение. Понятие атаки на информационную систему. Методы обеспечения информационной безопасности. Понятия безопасности. Безопасное использование социальных сетей. Характеристики и последствия угроз информации.

План

Угрозы информационной безопасности
Вредоносное ПО. Концепция атаки на информационную систему.
Методы обеспечения информационной безопасности
Безопасностьи концепции безопасности
Безопасное использование социальных сетей
Характеристики и последствия угроз информации

Информационная безопасность– это комплекс мер, направленных на обеспечение конфиденциальности, целостности и полезности информации.

Информационная безопасность включает в себя защиту информации от несанкционированного доступа, использования, раскрытия, чтения, копирования, изменения, уничтожения или искажения. Информационная безопасность охватывает технические, организационные и правовые аспекты и направлена на обеспечение стабильной работы информационных систем, защиты персональных данных и непрерывности бизнес-процессов.

Информационная безопасность- хранение и защита этой информации, а также системы и оборудование, предназначенные для ее использования, хранения и передачи.

Другими словами, представляющая собой набор технологий, стандартов и методов управления, необходимых для защиты информационной безопасности.

Что такое конфиденциальность информации?подразумевается, что доступ к информации имеют только уполномоченные лица или системы.

Это означает, что информация защищена от несанкционированного раскрытия, чтения или использования. Шифрование, контроль доступа, аутентификация и другие меры безопасности обеспечивают конфиденциальность, гарантируя, что информация будет доступна только тем, кому она нужна.

Что такое целостность информации?, понимается полнота, точность и достоверность информации.

Это означает, что информация защищена от несанкционированного изменения, уничтожения или повреждения. Для обеспечения целостности используются проверка данных, контроль версий, резервное копирование и другие меры безопасности, гарантирующие сохранность информации в её исходном состоянии.

> **Что такое вредоносное программное обеспечение?**, любое программное обеспечение, предназначенное для повреждения компьютерных систем, кражи данных, их компрометации или предоставления несанкционированного доступа. Сюда входят вирусы, черви, троянские программы, шпионское ПО, программы-вымогатели и другой вредоносный код.

Вредоносное ПО может нарушить работу системы, украсть личную информацию, привести к финансовому мошенничеству и вызвать множество других негативных последствий.

Примеры вредоносных программ:

1) Вирусы: они прикрепляются к другим файлам, заражают их и требуют вмешательства пользователя для распространения.

2) Черви: используют сети для распространения и размножения, могут распространяться без вмешательства пользователя.

3) Трояны: кажутся полезным программным обеспечением, но на самом деле наносят вред системе или крадут данные.

4) Шпионское ПО: отслеживает действия пользователя и крадет личную информацию.

5) Вредоносное ПО: шифрует пользовательские данные и требует выкуп за их разблокировку.

6) Рекламное ПО: постоянно показывает пользователю рекламу и может замедлить работу системы.

7) Руткиты: используются для сокрытия вредоносного ПО и глубокого проникновения в систему.

8)Кейлоггеры: записывают всю вводимую пользователем информацию, включая логины и пароли.

Эти программы представляют серьезную угрозу безопасности компьютера и требуют антивирусных программ и мер безопасности для защиты от них.

> **Что такое атака на информационную систему?**Под нарушением конфиденциальности, целостности или доступности информационной системы понимаются любые действия, направленные на нарушение

конфиденциальности, целостности или доступности информационной системы.

Эти атаки могут принимать различные формы, такие как распространение вредоносного ПО, кража данных, вывод системы из строя или попытка несанкционированного доступа. Атаки могут привести к сбою информационной системы, потере или повреждению данных, а также к финансовому и репутационному ущербу.

Обеспечение информационной безопасностиМетоды наращивания ресниц включают в себя:

1) Технические методы:

Антивирусное программное обеспечение: для обнаружения и устранения вредоносного программного обеспечения.

Межсетевые экраны: для блокирования несанкционированного доступа к системе.

Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS): для обнаружения и блокирования вредоносной активности.

VPN (виртуальная частная сеть): для обеспечения безопасного соединения через Интернет.

Шифрование: для защиты данных.

Многофакторная аутентификация (MFA): для защиты доступа к учетным записям.

2) Организационные методы:

Политики и стандарты безопасности: установление и соблюдение требований безопасности.

Обучение сотрудников: повышение осведомленности о рисках безопасности и обучение безопасному поведению.

Контроль доступа: ограничение прав доступа к данным.

Управление инцидентами: быстрое реагирование и разрешение инцидентов безопасности.

Постоянный мониторинг: Постоянный мониторинг безопасности системы.

3) Физические методы:

Защита серверной комнаты: предотвращение несанкционированного доступа.

Защита мест хранения данных: защита данных от кражи или уничтожения.

Обеспечение физической безопасности сотрудников: защита сотрудников от угроз.

4) Правовые методы:

Законы и нормативные акты: устанавливают правовые требования по обеспечению информационной безопасности.

Контракты: установите условия обмена информацией и включите требования безопасности.

Комплексное использование этих методов позволяет обеспечить высокий уровень информационной безопасности.

Хотя понятия «безопасность» и «защищенность» часто кажутся синонимами, они направлены на устранение разных рисков.

> **Когда вы говорите «Безопасность»**понимается состояние защищенности людей, имущества и окружающей среды от случайных опасностей.

Эти риски могут возникать в результате аварий, технических сбоев, стихийных бедствий или человеческих ошибок. Обеспечение безопасности включает в себя выявление рисков, их оценку и принятие мер по их предотвращению или снижению. Например, существуют правила и стандарты, направленные на обеспечение безопасности в таких областях, как безопасность дорожного движения, охрана труда, пожарная безопасность и других.

Под «безопасностью» обычно понимается защита от случайных опасностей, таких как аварии, стихийные бедствия или технические сбои.

> «Безопасность» означает защиту людей, имущества, данных и систем от преднамеренных угроз.

Эти риски могут быть вызваны преступностью, терроризмом, саботажем, шпионажем, кибератаками и другими злонамеренными действиями. Безопасность включает в себя выявление, оценку и принятие мер по предотвращению, снижению или реагированию на риски. Это может включать технические меры (например, камеры видеонаблюдения, системы сигнализации, межсетевые экраны), организационные меры (например, политики безопасности, контроль доступа, обучение персонала) и физическую защиту (например, охрану, барьеры). Целью безопасности является предотвращение или противодействие попыткам нарушения безопасности и минимизация последствий произошедших инцидентов.

«Безопасность» означает защиту от преднамеренных угроз, таких как преступность, терроризм или кибератаки.

Таким образом, в то время как «безопасность» направлена на снижение случайных рисков, «защищенность» направлена на предотвращение и борьбу с преднамеренными рисками.

> **Безопасное использование социальных сетей**Важно защищать свою личную информацию, обеспечивать безопасность своих учетных записей и внимательно следить за своим поведением в сети.

Ограничьте доступ к личной информации в настройках профиля, указав её только друзьям, используйте надёжные и уникальные пароли, включите двухфакторную аутентификацию и избегайте переходов по подозрительным ссылкам. Кроме того, будьте осторожны, делясь личной информацией с друзьями в интернете, немедленно сообщайте о кибербуллинге и домогательствах и позаботьтесь о своём психическом здоровье, ограничив время, проведённое в социальных сетях.

> **Характер угроз информации**может проявляться в различных формах, включая: вирусы, вредоносные программы, фишинг, кибератаки, кражу или уничтожение данных, а также злоупотребления со стороны внутренних сотрудников.

Последствия этих угроз могут быть серьёзными: финансовые потери, перебои в работе, потеря доверия клиентов, раскрытие персональных данных, ущерб репутации и даже юридическая ответственность. Именно поэтому важно защищать данные, внедрять меры безопасности и обучать сотрудников правилам безопасности.

Шаг 1: Определите характеристики угроз данным

Вредоносное ПО: включает вирусы, трояны, черви, программы-вымогатели и шпионское ПО. Они предназначены для повреждения компьютерных систем, кражи или шифрования данных.

Фишинг: это метод обмана людей с помощью поддельных электронных писем, веб-сайтов или сообщений с целью кражи личной информации (паролей, номеров банковских счетов и т. д.).

Кибератаки: к ним относятся DDoS-атаки (отказ в обслуживании), SQL-инъекции, межсайтовый скриптинг (XSS) и другие методы, которые используются для вывода из строя веб-сайтов, серверов и сетей или кражи данных.

Внутренние угрозы: включают несанкционированный доступ к данным, кражу или уничтожение данных сотрудниками. Это может произойти намеренно или случайно.

Социальная инженерия: это метод обмана, позволяющий заставить людей предоставить информацию или побудить их к совершению вредоносных действий.

Шаг 2: Проанализируйте последствия угроз

Финансовые потери: могут возникнуть в результате кражи данных, атак программ-вымогателей или кибератак. Они включают в себя сборы, штрафы, расходы на восстановление системы и простой бизнеса.

Перерыв в работе предприятия: может произойти в результате кибератак или системных сбоев. Это может привести к сбоям в обслуживании клиентов, остановке производства и снижению доходов.

Потеря доверия клиентов: это может произойти в результате утечек данных или кибератак. Это может привести к потере доверия клиентов к компании и переходу к другим компаниям.

Раскрытие личной информации: Личная информация клиентов, сотрудников или деловых партнеров может быть украдена или раскрыта. Это может привести к неправомерному использованию личной информации, нарушению конфиденциальности и юридической ответственности.

Репутационный ущерб: может возникнуть в результате кибератак, утечек данных или других инцидентов безопасности. Это может нанести ущерб репутации компании и негативно повлиять на её бизнес.

Юридическая ответственность: Нарушение законов о защите данных может повлечь за собой штрафы, судебные издержки и другие правовые санкции.

Шаг 3: Примите меры по защите от угроз

Разработайте и внедрите политику безопасности: эта политика определяет обязательства компании по защите данных и включает правила, процедуры и стандарты безопасности.

Использование технологий безопасности: к ним относятся межсетевые экраны, антивирусное программное обеспечение, системы обнаружения вторжений (IDS), системы предотвращения вторжений (IPS) и шифрование данных.

Обучите сотрудников вопросам безопасности: сотрудники должны знать о фишинге, социальной инженерии и других угрозах безопасности. Они должны научиться создавать надёжные пароли, быть бдительными к подозрительным письмам и следовать рекомендациям по защите данных.

Регулярные аудиты и оценки безопасности: необходимо проводить регулярные аудиты безопасности для выявления и устранения уязвимостей безопасности.

Разработайте план реагирования на инциденты: в случае возникновения инцидента безопасности необходимо разработать план быстрого и эффективного реагирования. Этот план должен включать

выявление инцидента, его устранение, восстановление систем и принятие мер по предотвращению подобных инцидентов в будущем.

Дополнительные материалы

Для успешного внедрения систем информационной безопасности на предприятии необходимо соблюдать три основных принципа:

1)Конфиденциальность ((Конфиденциальность).Предотвращать несанкционированное раскрытие информации в процессах ее создания, хранения, обработки, передачи и обмена, а также обеспечивать надлежащий уровень ее безопасности и конфиденциальности.

2) Целостность (целостность).Это предотвращает искажение и изменение информационного содержания.

3) Доступность - ДоступностьОна обеспечивает надежный и эффективный доступ к данным уполномоченным лицам. Восстановление системы после сбоя должно быть обеспечено таким образом, чтобы не оказывать негативного влияния на выполнение выполняемых в ней операций.

Логические (технические средства контроля).В ее основе лежит защита доступа к информационным системам, программное обеспечение, пароли, межсетевые экраны, а также контроль и управление доступом к информационным системам.

Различают следующие виды контроля:

- **Административный.**Административный контроль включает в себя утвержденные процедуры, стандарты и принципы. Законы и нормативные акты, принятые государственными органами, также являются видами административного контроля. Другими примерами административного контроля являются корпоративные политики безопасности, пароли и дисциплинарные взыскания.
- **Логические (технические средства контроля).**Средства логического (технического) контроля — информационные системы, программное обеспечение, пароли, межсетевые экраны, контроль доступа и управление информационными системами — основаны на защите доступа к информации.
- **Физик.**Контроль за рабочей средой и вычислительными устройствами.

Средства защиты информации подразделяются на:

- **Организационная поддержка.**Это совокупность организационно-технических (предоставление компьютерных возможностей, настройка кабельных систем и т.п.) и организационно-правовых (законодательная база, устав конкретной организации) средств.

- **Программное обеспечение**. Программы, помогающие управлять информацией, хранить и защищать ее, а также защищать доступ к ней.
- **Техническая (аппаратная) поддержка.**Это тип технического устройства, защищающего от несанкционированного доступа к информации.
- **Смешанное аппаратное и программное обеспечение**Они выполняют аппаратные и программные функции.

Технические средства защиты информации

Группа технических средств защиты информации объединяет аппаратные и программные средства.

Основные из них:

• регулярно создавать резервные копии важнейших массивов данных в компьютерной системе, а также использовать методы удаленного хранения;

• дублирование – копирование и резервное копирование всех подсистем сети, важных для информационной безопасности;

• Создание возможности перераспределения сетевых ресурсов в случае выхода из строя отдельных элементов сети;

• обеспечение наличия резервных систем электроснабжения;

• обеспечение безопасности оборудования от пожара и повреждения водой;

• установка программного обеспечения, защищающего от несанкционированного доступа к базам данных и другой информации.

Аутентификация и идентификация

Несанкционированный доступ к даннымДля исключения используются такие методы, как идентификация и аутентификация.

Идентификация- механизм присвоения уникального имени или изображения пользователю, который будет взаимодействовать с информацией.

Аутентификация– система методов проверки соответствия пользователя авторизованному уникальному имени или изображению.

Целью этих инструментов является разрешение или, наоборот, запрет доступа к информации.

Программные инструменты.Программные средства защиты информации — это система специальных программ, решающих задачу защиты информации.

Программы, обеспечивающие безопасность конфиденциальной информации, подразделяются на следующие направления:

Защита информации от несанкционированного доступа;

Защита информации от копирования;

Защита информации от вирусов;

Программная защита каналов связи.

Функции, выполняемые программными средствами защиты информации от несанкционированного доступа, включают в себя следующее:

1) Идентификация объектов и субъектов;

2) Установление ограничений доступа к вычислительным ресурсам и информационным ресурсам;

3) Мониторинг и регистрация действий с информацией и программами.

https://pirit.biz/reshenija/informacionnaja-bezopasnost

Типы средств защиты информации:

1)Антивирусные программы.

Компьютерный вирус- тип вредоносного программного обеспечения, создающего свои копии и внедряющего их в код других программ, области системной памяти и загрузочные сектора, а также распространяющего копии по различным каналам связи.

Существуют следующие типы вирусов:: Черви (глисты);Рекламное ПО (Рекламное ПО (ДТ); Шпионское ПО (Пират-шпион ДТ); Программы-вымогатели (Программы-вымогатели); Боты (Боты); Руткиты (Руткиты); Троянские программы (Троянские программы), Баги (Сумки)

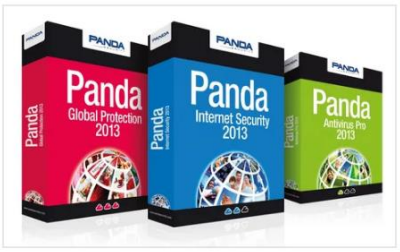
Антивирусные программы-Это программы, которые борются с компьютерными вирусами и восстанавливают поврежденные файлы.

2) Облачный антивирус - Облачный антивирус (CloudAV)

Одно из облачных решений по информационной безопасности, использующее легковесное программное обеспечение-агент для защиты защищаемых компьютеров и отправляющее анализ информации в инфраструктуру провайдера.

CloudAVвыполняет сканирование. Облачные антивирусы включают: Panda Cloud Antivirus, Crowdstrike, Cb Defense, Immunet, Bitdefender QuickScan, Comodo Cloud Antivirus, ESET Online Scanner, F-Secure Online Scanner, Kaspersky Security Scan, McAfee Security Scan Plus, Norton Security Scan, Panda Cloud Cleaner, Trend Micro HouseCall.

3) Data Leak Prevention (DLP) — это комплекс технологий,



направленных на предотвращение потери и распространения конфиденциальной информации на предприятиях по всему миру.

4) Криптографические системы — это системы преобразования информации, которые можно расшифровать только с помощью определённых кодов или шифров. Для этого**DES — стандарт шифрования данных**- Используется стандарт шифрования данных AES – Advanced Encryption Standard.

5) Межсетевые экраны (или брандмауэры) — это устройства контроля доступа к сети, предназначенные для блокирования и фильтрации сетевого трафика.

Межсетевые экраны(x)Межсетевые экраны обычно воспринимаются как сетевые или хостовые серверы. Сетевые межсетевые экраны располагаются в базовой сети на компьютерах-шлюзах локальных, глобальных и интранет-сетей.

6) VPN (Virtual Private Network) — виртуальная частная сеть. Это программа, позволяющая выделять и использовать частные сети среди сетей общего пользования для передачи и получения информации. Приложения, работающие в сети VPN, надёжно защищены. VPN позволяет удалённо подключаться внутри сети. С помощью VPN действия отдельных пользователей в сети защищаются (скрываются) с помощью прокси-серверов. С помощью VPN можно создать публичную сеть для географически удалённых предприятий.

7) Прокси-сервер (Proxy server)- это может быть конкретный компьютер или программа. Он действует как связующее звено между двумя устройствами, например, компьютером и другим сервером. Прокси-сервер может быть установлен на том же компьютере или на другом сервере совместно с межсетевым экраном. В приложениях, которые выполняют больше всего запросов, например, к интернет-сайтам, прокси-сервер кэширует их. Взаимодействие с прокси-сервером открывает возможности для поиска и устранения неполадок.

8) Системы мониторинга и управления информационной безопасностью, SIEMРешения SIEM используются для обнаружения и реагирования на угрозы информационной безопасности. SIEM-решение используется для сбора и анализа событий из различных источников, таких как межсетевые экраны, антивирусы, системы предотвращения вторжений (IPS) и операционные системы. Благодаря SIEM-системе компании могут централизованно хранить журналы событий.и с их помощью выявляются потенциальные угрозы, сбои в ИТ-инфраструктуре и кибератаки.

СИЭМПрограммы: VMware AirWatch,IBM MaaS360,Blackberry Enterprise Mobility Suite,VMware Workspace One

Контрольные вопросы:

Угрозы информационной безопасности

1) Что представляет собой угроза информационной безопасности?

2) Какие типы угроз существуют?

3) Каковы могут быть последствия утечки данных?

Вредоносное ПО

4) Что такое вредоносное ПО (вирус)?

5) Как вирусы заражают компьютер?

6) Что мне следует делать, чтобы защитить себя от вирусов?

Концепция атаки на информационную систему

7) Что такое атака на информационную систему?

8) Какова цель атак?

9) Как защититься от атак?

Методы обеспечения информационной безопасности

10) Каковы основные методы обеспечения информационной безопасности?

11) Как сохранить свой пароль в безопасности?

12) Зачем нужен брандмауэр?

Концепции безопасности

13) В чем разница между безопасностью и защищенностью?

14) Какой из пунктов больше связан с технической безопасностью?

15) Какой из них связан с безопасностью человека?

Безопасное использование социальных сетей

16) Какие правила безопасности следует соблюдать в социальных сетях?

17) С кем можно делиться личной информацией?

18) Что такое кибербуллинг?

Характеристики и последствия угроз информации

19) Какие угрозы существуют для данных?

20) Каковы могут быть последствия угроз?

Литература

1. Норалиев Н.Х., Расулов С.Ш.Учебник «Информационно-коммуникационные технологии». Ташкент, 2020. - 496 с.

2. Шоахмедова Н.Х., Абдуллаева И.М. «Информационно-коммуникационные технологии и системы в экономике» учебник. Ташкент, 2021. - 504 с.

3. Шыныбеков Д.А., Ускенбаева Р.К. и др. Информационно-коммуникационные технологии. 1-е изд. Учебник. Алматы, Издательство АО «Международный университет информационных технологий», 2017. - 559 с.

4. Браун и Г., Уотсон Д., «Кембриджский IGCSE ИКТ». Hodder Education, 3-е издание, 2021. — 571 стр.

5. Натан Марц, Джеймс Уоррен, «Принципы больших данных и передовой опыт масштабируемых систем обработки данных в реальном времени», Manning Shelter Island. 2015, - 330 страниц.

6. Урдушев Х., Мавлянов М., Эшанкулов С. Информационно-коммуникационные технологии в сфере. Часть I. Учебное пособие. – Самарканд: Издательско-полиграфический центр Самаркандского государственного университета ветеринарной медицины, животноводства и биотехнологии, 2024. 188 с.

7. Урдушев Х., Мавлянов М., Эшанкулов С. Информационно-коммуникационные технологии в сфере. Часть II. Учебное пособие. – Самарканд: Издательско-полиграфический центр Самаркандского государственного университета ветеринарной медицины, животноводства и биотехнологии, 2025. 200 с.

Информационные ресурсы Интернета

VMware AirWatch,IBM MaaS360,Blackberry Enterprise Mobility Suite,VMware Workspace One

https://www.securitylab.ru/news/529985.phpМагнитные вихри можно использовать для генерации случайных долот.

https://searchinform.ru/informatsionnaya-bezopasnost/zaschita-informatsii/sposoby-zaschity-informatsii/

Способы защиты информации | Методы информационных технологий - СёрчИнформ

https://studopedia.ru/11_70142_programmnie-sredstva-zashchiti-informatsii.html Программные средства защиты информации — Студопедия

Мисти Э. Вермаат, Сьюзен Л. Себок, Стивен М. Фройнд. Дженнифер Т. Кэмпбелл, Марк Фрайденберг. «Открывая компьютеры: инструменты, приложения, устройства и влияние технологий» (учебник). Cengage Learning. Channel Center Street, 20. Бостон, Массачусетс, 02210. США, 2016.

Романова Ю.Д., Лесничая И.Г., Шестаков В.И., Пропавший без вести И.В., Музычкин П.А. Информатика и информационные технологии: учебное пособие / под ред. Ю.Д.Романовой.-3-е изд., перераб. и доп.-М.: Эксмо, 2008.