**Слайд 2**

Сегодня информационная безопасность — это не просто защита компьютеров и сетей, а целый комплекс научных и технических подходов, которые обеспечивают сохранность, доступность и целостность информации. С развитием технологий мы сталкиваемся с растущими объёмами данных и всё более изощрёнными угрозами, поэтому возникает необходимость в более точных, количественных методах анализа информационных потоков. Одним из таких методов и является **энтропийный подход**.

Понятие **энтропии** пришло в информационную безопасность из других областей науки — в первую очередь из физики и теории информации. В этих дисциплинах энтропия означает степень неопределённости или хаотичности системы. Перенеся это понятие в область информационной безопасности и автоматизированных систем, мы получили мощный инструмент для оценки сложности, случайности и потенциальной уязвимости данных.

Зачем это нужно? Дело в том, что большинство методов защиты информации опираются на предположение о случайности — будь то генерация паролей, криптографических ключей или даже структура сетевого трафика. Если эта «случайность» поддельная, шаблонная или предсказуемая — система может быть скомпрометирована. Энтропия позволяет **количественно** измерить, насколько «непредсказуемыми» и, следовательно, надёжными являются те или иные данные.

**Слайд 3**

Чтобы понимать значение энтропии, нужно сначала обратиться к основам теории информации.  
Информация — это, по сути, уменьшение неопределённости. Если мы точно знаем, что произойдёт, — мы не получаем никакой информации от любых сообщений. Но если результат непредсказуем (неизвестен) — тогда каждое новое знание даёт нам информацию.  
**Информацию Шеннон определил как снятую неопределённость – результат выбора одного варианта из числа возможных, уменьшение количества рассматриваемых вариантов (разнообразия).**

**Слайд 4**

Как уже говорилось, энтропия — это мера неопределённости или, иначе говоря, мера количества информации, которую содержит сообщение или источник данных. Чем выше энтропия, тем менее предсказуемы данные, и тем сложнее их анализировать или предугадать.

Интуитивно можно сказать, что энтропия показывает, насколько «хаотично» ведёт себя источник информации. Если мы имеем дело с очень упорядоченной последовательностью, например, «00000000», то она содержит минимум информации и имеет энтропию, близкую к нулю. Если же перед нами случайная последовательность вроде «10011010», энтропия будет значительно выше, потому что каждое следующее значение трудно предсказать.

С математической точки зрения, энтропия для дискретного источника определяется формулой Шеннона, которую мы уже упоминали:

Где p(i)— вероятность появления i-го символа (или события) в выборке данных.

N — количество уникальных символов (или возможных состояний), которые могут быть в данных.

Эта формула даёт значение в битах, отражающее среднее количество информации на один символ.

Пример: если символы появляются равновероятно — например, в алфавите из 4 символов каждый встречается с вероятностью 0.25 — энтропия будет максимальной: H=2 бита. Если же один символ встречается почти всегда, а остальные — редко, энтропия будет ниже.

**Слайд 5**

Что такое энтропия простым языком? Давайте представим, что у нас есть коробка с шариками разных цветов: красные, синие и зеленые. Если в коробке много красных шариков и всего несколько синих и зеленых, то мы можем легко угадать, какого цвета шарик мы достанем. В этом случае энтропия низкая, потому что информация о цвете шарика предсказуема.

Теперь представим, что в коробке шариков примерно одинаковое количество всех цветов. В этом случае, когда мы достаем шарик, нам будет сложнее угадать его цвет, потому что шансы на каждый цвет равны. Здесь энтропия высокая, потому что информация о цвете шарика менее предсказуема.

В информационных системах энтропия помогает оценить, насколько данные разнообразны и сложны. Чем выше энтропия, тем больше информации мы можем извлечь из системы, и тем сложнее ее понять. Это важно, например, в криптографии, где мы хотим, чтобы наши сообщения были трудными для расшифровки.

Важный момент: энтропия не измеряет «качество» информации, она лишь характеризует её структуру с точки зрения предсказуемости.

Существует также понятие условной энтропии, когда мы измеряем количество информации при условии, что часть уже известна. Оно особенно важно при анализе зависимостей между событиями, например, в моделях прогнозирования поведения пользователя или выявления аномалий.

Кроме того, важно различать теоретическую энтропию — которую можно вычислить, зная вероятности заранее, — и оценочную, которую получают эмпирически, анализируя реальные данные. Именно последняя активно применяется в информационной безопасности для анализа трафика, логов и содержимого файлов.

Таким образом, энтропия — это не просто абстрактное понятие, а мощный инструмент, позволяющий количественно оценить степень хаотичности или закономерности в данных.

**Слайд 6**

Энтропия в информационной безопасности — это практический инструмент для оценки надёжности систем и обнаружения угроз.

1. **Энтропия как мера случайности**: Важна при генерации криптографических ключей и данных, чтобы они были непредсказуемыми и трудными для взлома.
2. **Обнаружение аномалий и атак**: Снижение энтропии в трафике может сигнализировать о вредоносной активности или аномалиях, например, при DDoS-атаках.
3. **Обнаружение вредоносного ПО**: Вредоносное ПО часто использует обфускацию, увеличивая энтропию, что затрудняет его обнаружение.
4. **Оценка рисков и уязвимостей**: Высокая энтропия паролей и данных означает большую безопасность, низкая — уязвимость к атакам.
5. **Сетевая безопасность и защита от вторжений**: Анализ энтропии сетевого трафика помогает выявлять аномалии, например, при попытках вторжения или взлома.

**Слайд 7**

Энтропия играет ключевую роль в криптографии, обеспечивая безопасность алгоритмов шифрования и криптографических ключей. Чем выше энтропия, тем сложнее предсказать ключ или взломать систему.

Например:

1. **Генерация криптографических ключей**: Ключи должны быть случайными, с высокой энтропией, чтобы система оставалась стойкой к атакам.
2. **Генерация случайных чисел**: Для криптографических систем важно, чтобы случайные числа, используемые для ключей, имели высокую энтропию, исключая их предсказуемость.

**Слайд 8**

Пароль является самым распространённым методом аутентификации в информационных системах.

Однако пароли с низкой энтропией легко поддаются различным атакам, например, атакам методом перебора (brute force) или атакам по словарю.

Чем выше энтропия пароля, тем сложнее для злоумышленников угадать его.

Пример:

Рассмотрим два пароля:

Пароль с низкой энтропией: «password123»

Пароль с высокой энтропией: «W#v$8zL*7n@2Q»*

*Пароль «password123» имеет очень низкую энтропию, потому что состоит из распространённого слова и чисел, что делает его уязвимым для атак по словарю. Злоумышленники могут быстро подобрать такой пароль, используя заранее подготовленный список популярных паролей.*

*С другой стороны, пароль «W#v$8zL*7n@2Q» обладает гораздо большей энтропией, потому что включает случайные символы, большие и маленькие буквы, цифры и специальные знаки, что существенно увеличивает количество возможных вариантов. В этом случае, атаки методом перебора требуют гораздо больше времени и вычислительных ресурсов, что значительно повышает безопасность системы.

**Слайд 9**

Энтропия играет важную роль не только в криптографической защите, но и в области **обнаружения вторжений**. В этом контексте она используется для выявления аномалий в сетевых потоках и системах, которые могут указывать на попытки вторжения или другие виды зловредной активности. Высокая энтропия часто ассоциируется с нормальной случайной активностью, в то время как резкие изменения в энтропийных показателях могут свидетельствовать о нарушениях.

**Слайд 10**

Энтропия играет ключевую роль в современных автоматизированных системах, особенно в тех, которые предназначены для мониторинга, анализа и принятия решений в условиях неопределенности. В таких системах она используется как метрика, отражающая степень хаоса или неожиданности во входных данных. Это позволяет системе реагировать на отклонения от нормы и адаптироваться к изменяющимся условиям в реальном времени.

С помощью оценки энтропии автоматизированные системы могут:

* выявлять **аномалии в потоках данных**, что критически важно для систем обнаружения вторжений (IDS) и предотвращения атак (IPS);
* **отслеживать сбои и нестабильность** в функционировании аппаратного или программного обеспечения;
* **принимать решения на основе анализа неопределенности**, позволяя системе гибко реагировать в условиях дефицита информации.

Высокий уровень энтропии, зафиксированный в потоке данных, может свидетельствовать о таких инцидентах, как:

* появление **вредоносного трафика** или подозрительной активности;
* **сбой работы датчиков** или некорректное поведение оборудования;
* резкое изменение пользовательской активности, которое может говорить о **внутренней угрозе** или компрометации системы.

**Слайд 11**

В различных отраслях автоматизированные системы, использующие анализ энтропии, демонстрируют высокую эффективность.

* **Системы обнаружения вторжений (IDS/IPS):** анализ энтропии сетевых пакетов позволяет выявлять необычные паттерны, например, спайк в количестве нестандартных пакетов, что может указывать на атаку типа DDoS или сканирование портов.
* **Алгоритмы сжатия данных:** использование энтропии позволяет оценить степень сжимаемости информации. Чем выше энтропия — тем менее предсказуема информация, и тем сложнее её эффективно сжать. Это помогает оценивать эффективность алгоритмов архивации и оптимизировать хранилища.
* **Машинное обучение:** энтропия используется для оценки неопределенности модели. Это позволяет отсеивать сомнительные предсказания, принимать решения о необходимости запроса дополнительной информации и т.д.
* **Интернет вещей (IoT):** в распределённых устройствах энтропия сигналов помогает обнаруживать поломки, нестабильную работу, вторжения в сеть.
* **Робототехника:** автономные системы (дроны, роботы, манипуляторы) используют энтропию для оценки неопределенности окружающей среды. Это позволяет корректировать курс, избегать препятствий, а также адаптировать поведение к новым условиям — особенно важно в условиях частичной или шумной информации.

**Слайд 12**

Использование энтропии в автоматизированных системах, несмотря на свою полезность, сталкивается с несколькими проблемами и ограничениями. Одной из главных проблем является высокий уровень ложных срабатываний, когда повышение энтропии может быть вызвано нормальными изменениями, такими как пик трафика или изменение поведения пользователей. Это может привести к ненужным мерам безопасности, например, блокировке пользователей. Также энтропийный анализ сильно зависит от качества данных: ошибки или шум могут исказить результаты и привести к неправильным выводам. В реальных системах, работающих с большими объемами данных в реальном времени, требуется значительная вычислительная мощность, что может замедлить обработку и снизить производительность.

Особое внимание необходимо уделить **генераторам случайных чисел (ГСЧ)** — важному элементу криптосистем. Даже если система в целом показывает высокую энтропию, **предсказуемость или уязвимость ГСЧ полностью компрометирует безопасность**. В реальности нередко используются некачественные или устаревшие ГСЧ, в результате чего ключи, токены и другие криптографические параметры становятся уязвимыми к атаке.

Энтропия также имеет ограничения в применении, особенно в случае целенаправленных атак или DDoS-атак, где изменение энтропии может быть минимальным или неинформативным. Несмотря на эти проблемы, правильное сочетание энтропийного анализа с другими методами может повысить точность и эффективность систем безопасности и мониторинга.

**Слайд 13**

Энтропия имеет большие перспективы в области информационной безопасности, особенно с учетом роста объемов данных и угроз. Одним из главных направлений является использование энтропии в квантовых вычислениях для улучшения безопасности криптографических протоколов и оценки случайности квантовых ключей.

**Например, энтропия может быть эффективно интегрирована в SIEM-системы (Security Information and Event Management).** Эти системы собирают, коррелируют и анализируют события безопасности из различных источников в реальном времени. Встраивание энтропийного анализа в SIEM позволяет **оперативно выявлять аномалии в поведении пользователей, сетевом трафике и логах,** усиливая возможности реагирования и снижая время на обнаружение атак.

Кроме того, в биометрической безопасности энтропия способствует улучшению точности аутентификации и защите от фальсификаций. В будущем энтропия будет играть ключевую роль в автоматических системах защиты информации, позволяя динамично реагировать на изменения угроз и активности. Эти перспективы делают энтропию важным инструментом для дальнейших инноваций в сфере безопасности данных и защиты технологий.

**Слайд 14**

Энтропия играет ключевую роль в информационной безопасности и автоматизированных системах, выступая мерой неопределённости и случайности. Она лежит в основе криптографии, генерации надёжных паролей и ключей, а также анализа сетевого трафика и выявления аномалий. Несмотря на существующие ограничения, энтропийные методы остаются важным инструментом защиты информации и продолжают развиваться в условиях роста угроз и цифровизации.