MOXA®

Что необходимо знать о кибербезопасности?

Основные понятия

Основные понятия в кибербезопасности, которые вы должны знать.

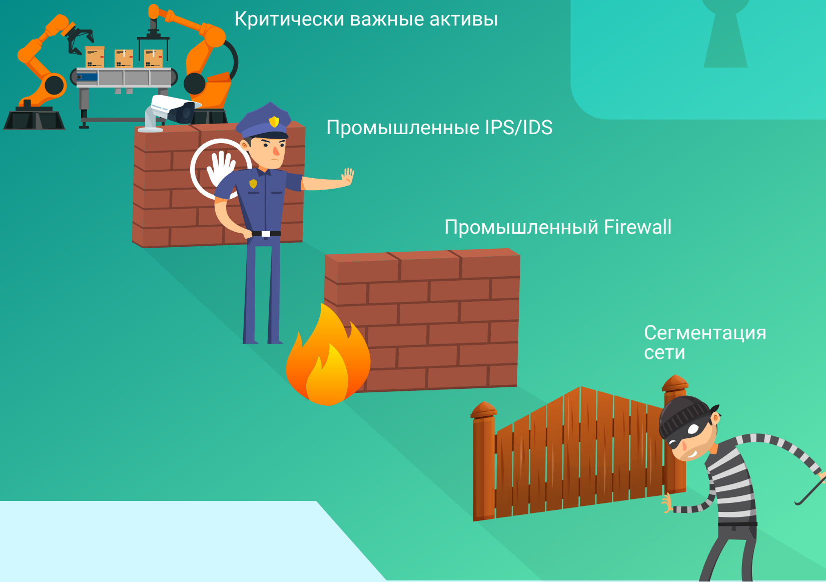
Понимание общей терминологии в области кибербезопасности может помочь вам обсудить важные вопросы с IT-специалистами.

Концепция	Защитные механизмы	Угрозы
Defense in Depth (глубокая защита)	**Firewall**	Вредоносное ПО
	IDS (Система обнаружения вторжений)	Вирусы-вымогатели
	IPS (Система предотвращения вторжений)	DoS/DDoS-атаки
	DPI (Инспекция пакетов)	

Defense in Depth

Архитектура Defense in Depth

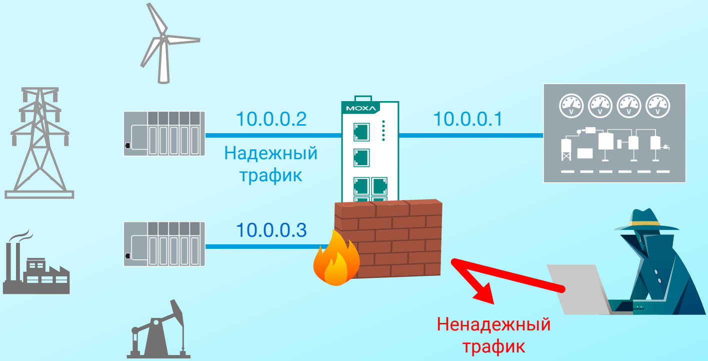
Концепция основана на нескольких механизмах безопасности, находящихся на разных уровнях. Если один из механизмов выйдет из строя, другие продолжат функционировать в качестве резервных. Такая стратегия позволяет повысить безопасность системы в целом, и промышленная сеть все равно будет достаточно защищена от возможных угроз.



Промышленный Firewall

Промышленные межсетевые экраны контролируют трафик, приходящий в сеть извне и выходящий из нее.

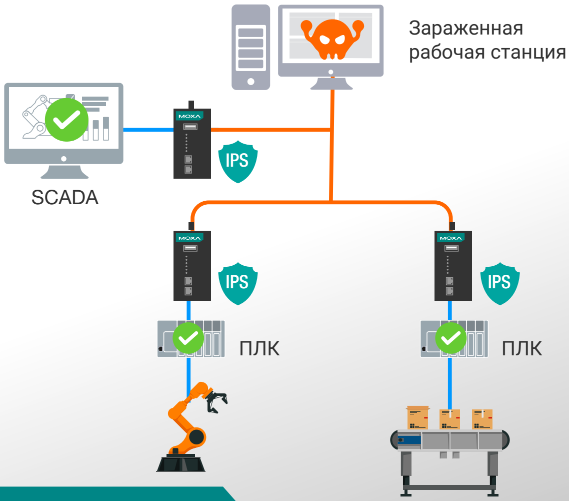
Их основной задачей является защита сегментов сети от несанкционированного доступа, поэтому чаще всего их размещают на границе сети и между различными ее сегментами. Защита осуществляется посредством обнаружения и фильтрации нежелательного трафика – его промышленные межсетевые экраны ограничивают на основе определенного набора правил безопасности (в соответствии с заданными шаблонами).



Промышленная IPS

Промышленная система предотвращения вторжений

Промышленная IPS – это устройство или целая система, которые не только идентифицируют вредоносную активность, регистрируют информацию о ней и оповещают об этом событии, но еще и пытаются заблокировать или остановить угрозу. Информацию о полезных данных промышленные IPS получают с помощью инспекции пакетов (DPI).

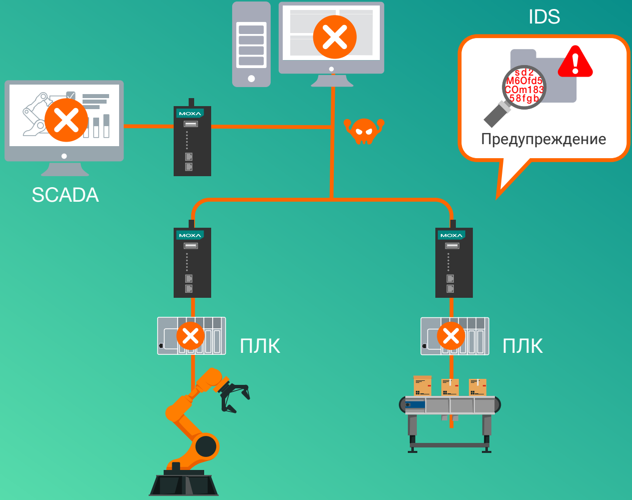


Промышленная IDS

Промышленная система обнаружения вторжений

Промышленная IDS - это устройство или целая система, которые отслеживают сетевой трафик на предмет подозрительной активности и выдают предупреждение при обнаружении таковой.

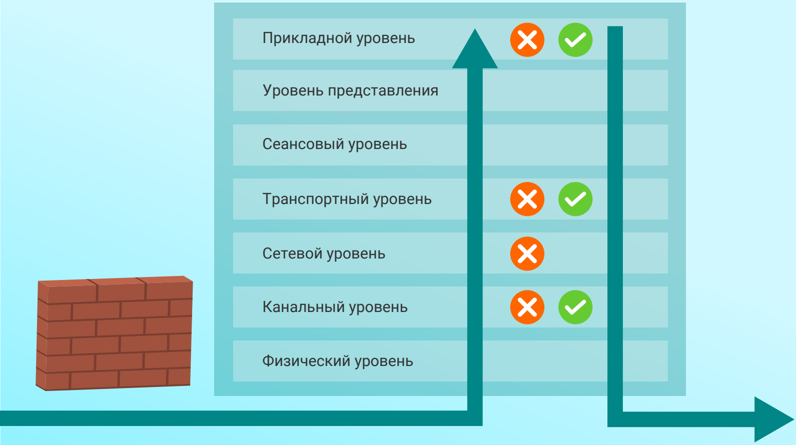
Зараженная
рабочая станция



DPI

Deep Packet Inspection

Усовершенствованный метод проверки и управления сетевым трафиком на прикладном уровне сетевой модели OSI на основе содержимого сетевых пакетов. Технология DPI интегрирована с IT-OT, это означает, что она способна распознавать протоколы как IT, так и АСУ ТП. Данный метод эффективен для мониторинга и предотвращения DoS-атак и защиты от вредоносных программ.



Прикладной уровень ✗ ✓

Уровень представления

Сеансовый уровень

Транспортный уровень ✗ ✓

Сетевой уровень ✗

Канальный уровень ✗ ✓

Физический уровень

Вредоносное ПО

Вредоносное программное обеспечение

Общее название любого программного обеспечения, специально предназначенного для нанесения ущерба компьютеру, пользователю или целой компьютерной сети, приводящего к снижению производительности компьютера или системы.

Вирус

фрагмент кода, который воспроизводит сам себя. Распространяется действиями пользователя, может быть передан с одного компьютера на другой.

Червь

вредоносная программа, которая распространяется автоматически.

Троян

вредоносное ПО, которое маскируется под легальное программное обеспечение.

Руткит

программы, использующиеся для прикрытия хакерских действий. Прячутся глубоко внутри ПК.

Шпионское ПО

следит за пользовательской активностью, собирает данные (пароли, номера кредитных карт и т.п.) и отправляет их стороннему лицу.

Удаленный доступ

удаленное управление устройствами.

Рекламное ПО

зловредная программа, которая навязчивым образом отображает нежелательные рекламные объявления.

Программы-вымогатели

зловредное ПО, которое зашифровывает пользовательские файлы или блокирует доступ к системе, а после просит выкуп за восстановление данных.

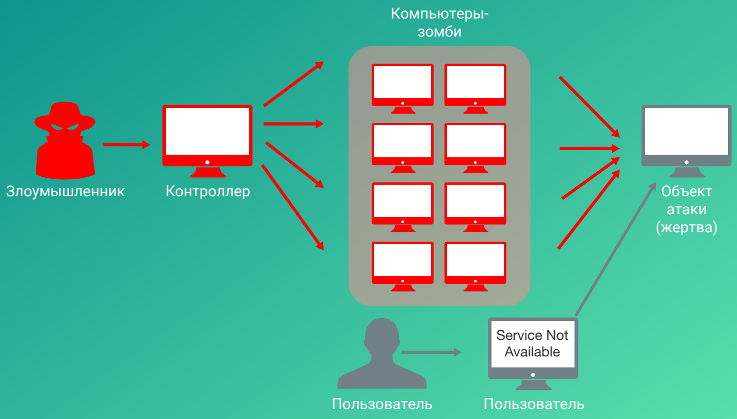
Случаи кибератак

- ! Программа-вымогатель нанесла вред ведущему производителю чипсетов, в результате чего убытки компании составили 170 миллионов долларов США.
- ! Ущерб от программы-вымогателя LackerGoga в 2019 году превысил 40 миллионов долларов США.

DoS/DDoS-атаки

Отказ в обслуживании (DoS) и Распределенный отказ в обслуживании (DDoS)

DoS – это атака, предназначенная для прекращения работы компьютеров или сети, что делает их ресурсы недоступным для предполагаемых пользователей. Это может быть достигнуто путем наводнения объекта атаки трафиком или отправки информации, которая вызывает сбой. DDoS-атака выполняется одновременно с множества компьютеров и имеет такую же цель – привести к отказу системы.



Комплексная безопасность
сегментов АСУ ТП и IT

Защитите свою промышленную сеть

Компания Moxa разработала промышленные решения для обеспечения должного уровня кибербезопасности, которые включают в себя важнейшие технологии и концепции информационной кибербезопасности, такие как система предотвращения вторжений (IPS) и другие, которые создавались специально для защиты АСУ ТП от киберугроз, при этом они не вмешиваются в промышленные операции и процессы.

Подробнее:
https://moxa.ru/landing/Cybersecurity-Microsite/index.htm

MOXA®

www.moxa.ru