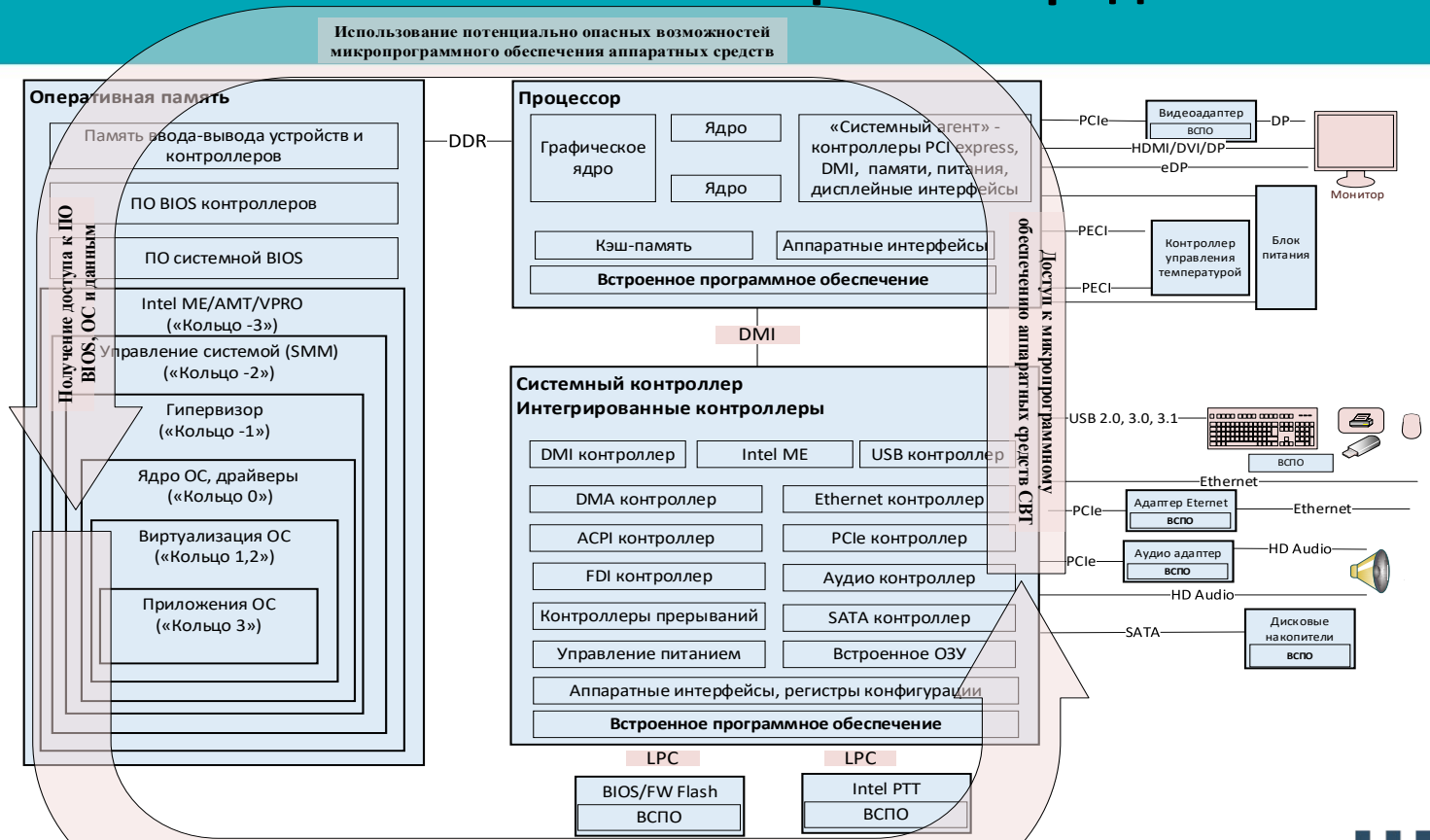
Микропрограммное обеспечение аппаратных средств - напоминание об угрозах

Аксененко Юрий Иванович

ЦБИ Центр безопасности информации

Вектор реализации угроз, связанных с микропрограммным обеспечением аппаратных средств СВТ



Получение доступа к ПО BIOS, ОС, ППО и данным

Использование возможностей микропрограммного обеспечения аппаратных средств СВТ

Доступ к микропрограммному обеспечению аппаратных средств СВТ

Удаленный запуск произвольного кода и (или) несанкционированный доступ к информации в обход средств защиты информации, в том числе встроенных в операционные системы и виртуальные машины
УБИ.195, УБИ.092У, БИ.010 У

Поддержка технологии DMA.
Наличие «свободных», в том числе скрытых областей памяти, и избыточной функциональности.
Возможность организации скрытых каналов управления и «внеполосного» обмена информацией.
Возможность «непосредственного» чтения (записи) произвольных областей памяти микроконтроллеров.

Внедрение вредоносного кода в микропрограммное обеспечение в процессе разработки, поставки и пр.

Использование технологии Intel ME для доступа к микропрограммному обеспечению
УБИ.092

Запуск вредоносной программой собственного гипервизора, загрузка нештатной операционной системы
УБИ.010, УБИ.018

Отключение или вывод из строя отдельных устройств ПЭВМ, включая средства хранения, обработки, ввода/вывода/передачи информации, путем отправки специально сформированных команд, несанкционированного переконфигурирования BIOS
УБИ.024, УБИ.143, УБИ.180

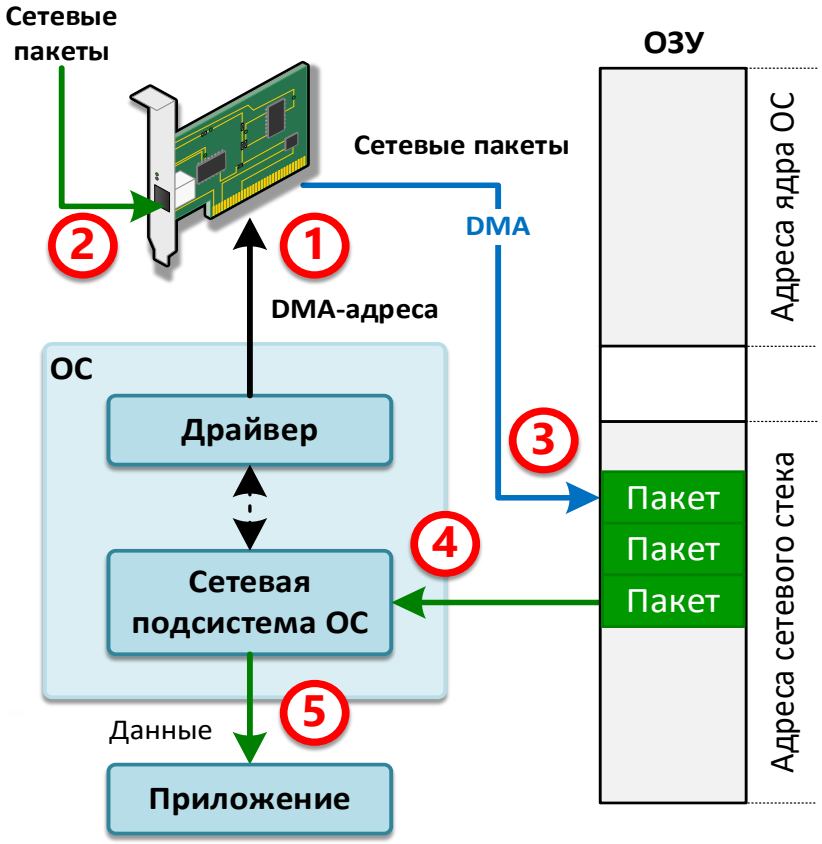
Установка обновления микропрограммного обеспечения, содержащего вредоносный код
УБИ.005

Несанкционированное «внеполосное» подключение к ПЭВМ и ее устройствам
УБИ.092

Восстановление старой версии BIOS, которая может содержать уязвимости, или установка уязвимой версии BIOS
УБИ.009, УБИ.032

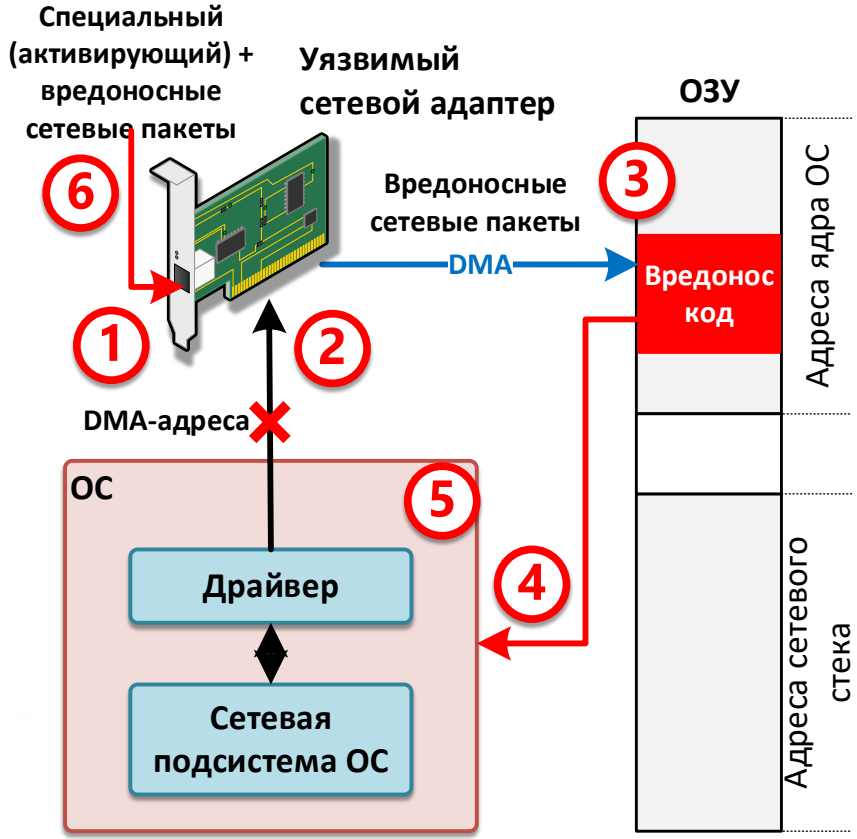
Несанкционированный доступ из операционной системы к к ядру процессора и микропрограммному обеспечению, в том числе для эксплуатации уязвимостей процессоров и микропрограммного обеспечения и(или) внедрения вредоносного кода в микропрограммное обеспечение, путем удаленного или локального подключения к операционной системе, использования штатных функций ОС и (или) вредоносного программного обеспечения, установленного в операционной системе
УБИ.N01, УБИ.143, УБИ.195, УБИ.N01, УБИ.195, УБИ.N01, УБИ.072, УБИ.011, УБИ.010, УБИ.072

Типовая схема приема сетевых пакетов



1. Инициализация адресов ОЗУ для приема пакетов
2. Прием сетевого пакета сетевым адаптером
3. Запись сетевого пакета в ОЗУ по DMA-каналу
4. Чтение пакета из ОЗУ для обработки
5. Передача данных сетевого пакета приложению

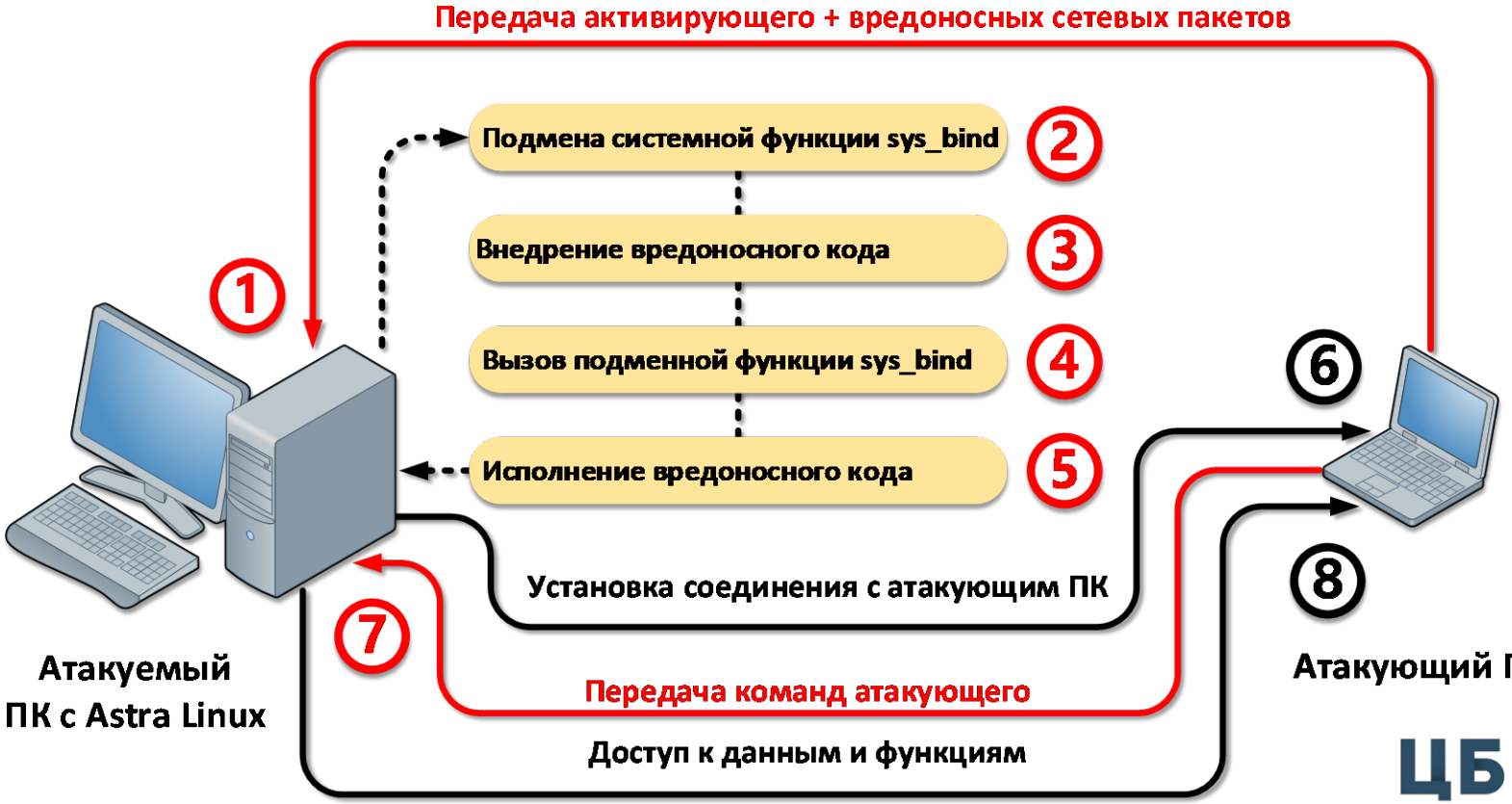
Эксплуатация уязвимости сетевого адаптера



1. Прием активирующего и вредоносных пакетов
2. Игнорирование DMA-адресов от драйвера
3. Запись вредоносного кода в область ОЗУ ядра ОС
4. Выполнение вредоносного кода
5. Нарушение безопасности функционирования ОС
6. Возможность получения нарушителем полного доступа к данным и функциям

ЦБИ Центр безопасности информации

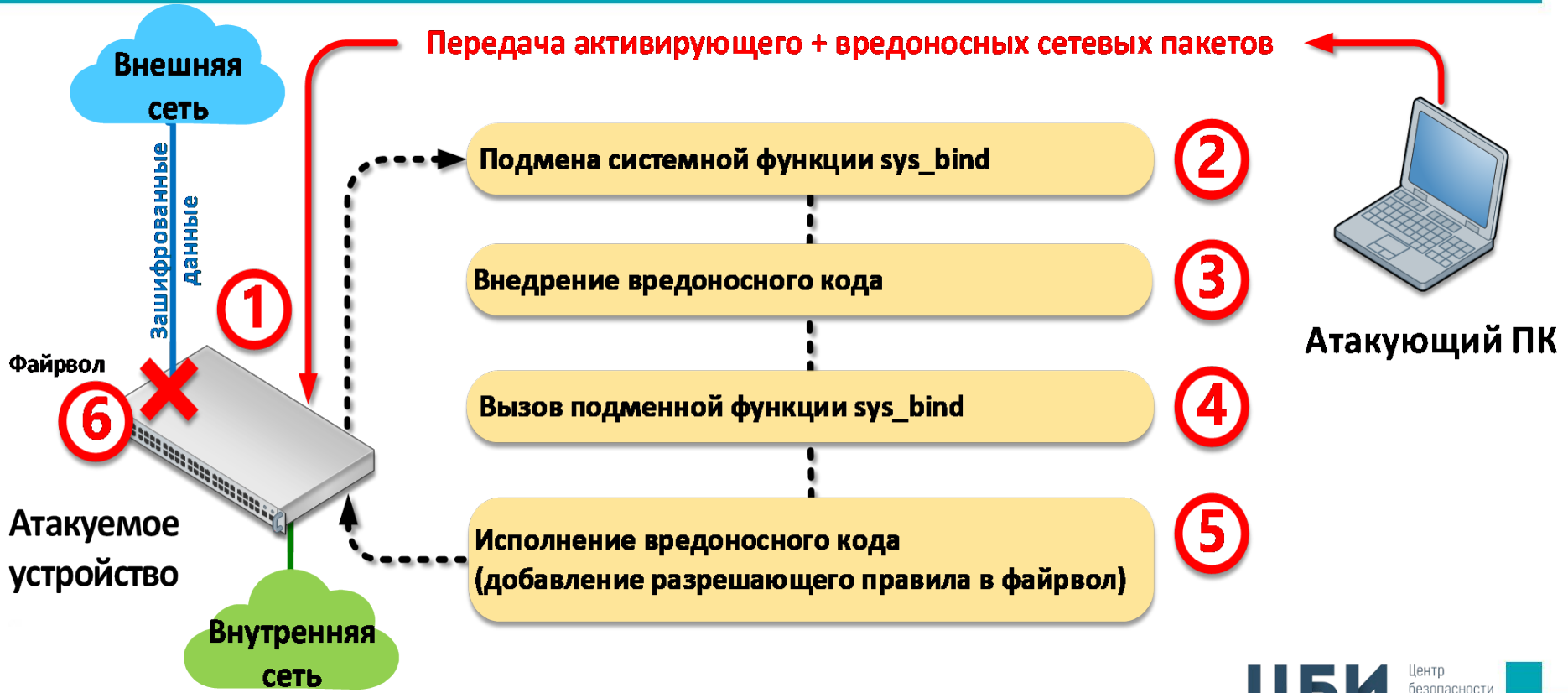
Атака на Linux



ЦБИ Центр безопасности информации

Атака на криптомаршрутизатор

Этап 1. Добавление решающего правила в файрвол



Атака на криптомаршрутизатор

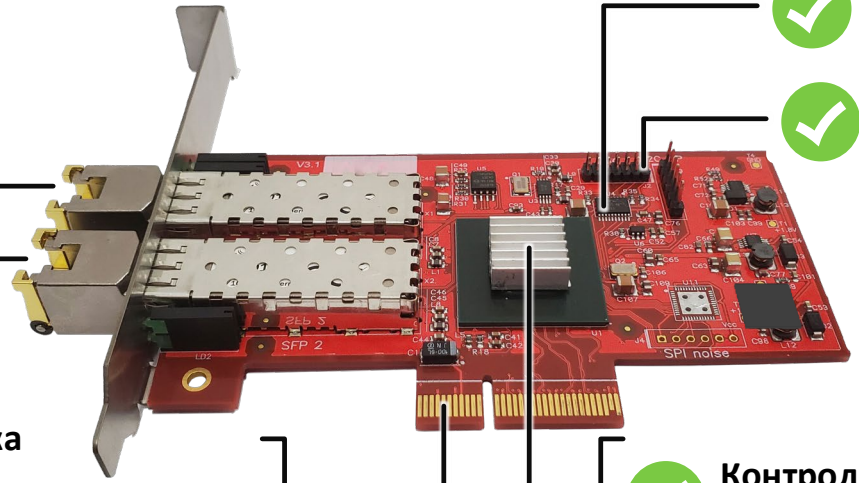
Этап 2. Получение доступа к зашифрованным данным

Доверенный сетевой адаптер «TrustNet»

Ограничение доступа через сетевые интерфейсы к оперативной памяти СВТ только в разрешенном диапазоне адресов

- ✗ Настройка
- ✗ Изменение встроенного ПО
- ✓ Фильтрация сетевых пакетов

- ✗ Настройка
- ✗ Изменение встроенного ПО
- ✓ Маскирование данных



- ✓ Хранение правил фильтрации
- ✓ Настройка

- ✓ Контроль целостности встроенного ПО
- ✓ Контроль обращений к ОЗУ

Исключение возможности доступа к оперативной памяти СВТ со стороны сетевого интерфейса за пределами разрешенного диапазона адресов

Что еще полезного мы можем и должны сделать?

Корректировка нормативного обеспечения в части уточнения критериев и требований доверия к микропрограммному обеспечению.
Разработка методологии подтверждения требований доверия.

Определение наиболее критичных компонент СВТ.
Разработка и сертификация доверенных компонент СВТ

Разработка мер, компенсирующих «недостаток» доверия.