POSITIVE TECHNOLOGIES

Игра в рулетку, или
Как выбирать средства защиты

Наталья Куканова

Positive Technologies

Ведущий эксперт

Образовательная программа «Практическая безопасность»

Что такое анализ рисков?

Выбор оптимального решения с учетом всех возможных факторов.

- Доделать всё сегодня или завтра прийти пораньше?
  - «Завтра приду пораньше, а сегодня вечером встречусь с друзьями. С другой стороны, если я встречусь с друзьями, то пораньше не приду…»
- Куда поехать в отпуск?
  - «Европа безопаснее, но зато Азия интереснее. А может, к маме в деревню? Там пирожки и варенье…»
- Проскочить на «светло-зелёный» или подождать зелёного?
  - «Везде успевает тот, кто никуда не торопится. Подожду зелёного…»
- Какой институт выбрать для ребенка?
  - «А может, пусть он сам себе институт выбирает?..»

Анализ рисков в ИБ

Цель — выбрать оптимальный набор средств защиты ИС.

Механизм — анализ рисков.

Важные факторы:

- ценность информации;
- угрозы и уязвимости ИС.

Идеальная картина. То, чего не может быть

— Методика анализа рисков определена и описана.

— Ценность данных определена.

— Угрозы и уязвимости выявлены.

— Риски определены и оценены.

— Средства защиты выбраны, приобретены, установлены и настроены.

Всё работает!

А в реальности…

— Владелец информации о ее ценности: «Ну, пишите второй уровень… Потому что он средний. А так вообще я не знаю, что писать».

— Поверхностный аудит выявил не более половины уязвимостей, а на кропотливый аудит не выделен бюджет.

— «Давайте везде поставим антивирусы и межсетевые экраны, потому что ~~слова знакомые~~ это важно».

Сложности

— Инвентаризация информационных ресурсов не проводится или проводится нерегулярно.

— Владельцам сложно определить ценность своей информации — даже при наличии методики.

— Кропотливый аудит, выявляющий большинство угроз и уязвимостей, требует значительного объема ресурсов.

— Регулярный процесс анализа рисков не поддерживается.

О чем мой рассказ

— Как определить уровень зрелости компании и зачем его определять?

— Почему важно не пытаться реализовать «классический» анализ рисков так, как написано в учебниках, если компания к этому не готова?

— Как найти максимально удобный механизм выбора мер защиты — вместо анализа рисков?

Модель зрелости

Модель зрелости согласно COBIT

№	Наименование	Состояние процессов управления рисками
0	Нулевой	Не применяются
1	Начальный	Процесс используется разово или в отдельных случаях и не организован
2	Повторяемый	Процесс повторяется по образцу
3	Определенный	Процесс документально оформлен и доведен до сведения участвующих сторон
4	Управляемый	Ведется мониторинг процесса в измеряемых показателях
5	Оптимизированный	Лучшие практики внедрены и автоматизированы

Подходы к определению средств защиты

Уровень зрелости	IT-процессы	Бизнес-процессы
Низкий (Base)	IT-процессы не построены. Все происходит «само собой» по инициативе отдельных сотрудников	Бизнес-процессы не формализованы. Владельцы процессов не назначены
Средний (Advanced)	Некоторые IT-процессы работают, но не документированы; нет мониторинга и контроля	Бизнес-процессы определены, но не классифицированы
Высокий (Risk Analysis)	Большинство процессов описаны и выполняются, организован контроль над их исполнением	Бизнес-процессы определены, описаны и классифицированы по степени важности

Подходы к определению средств защиты

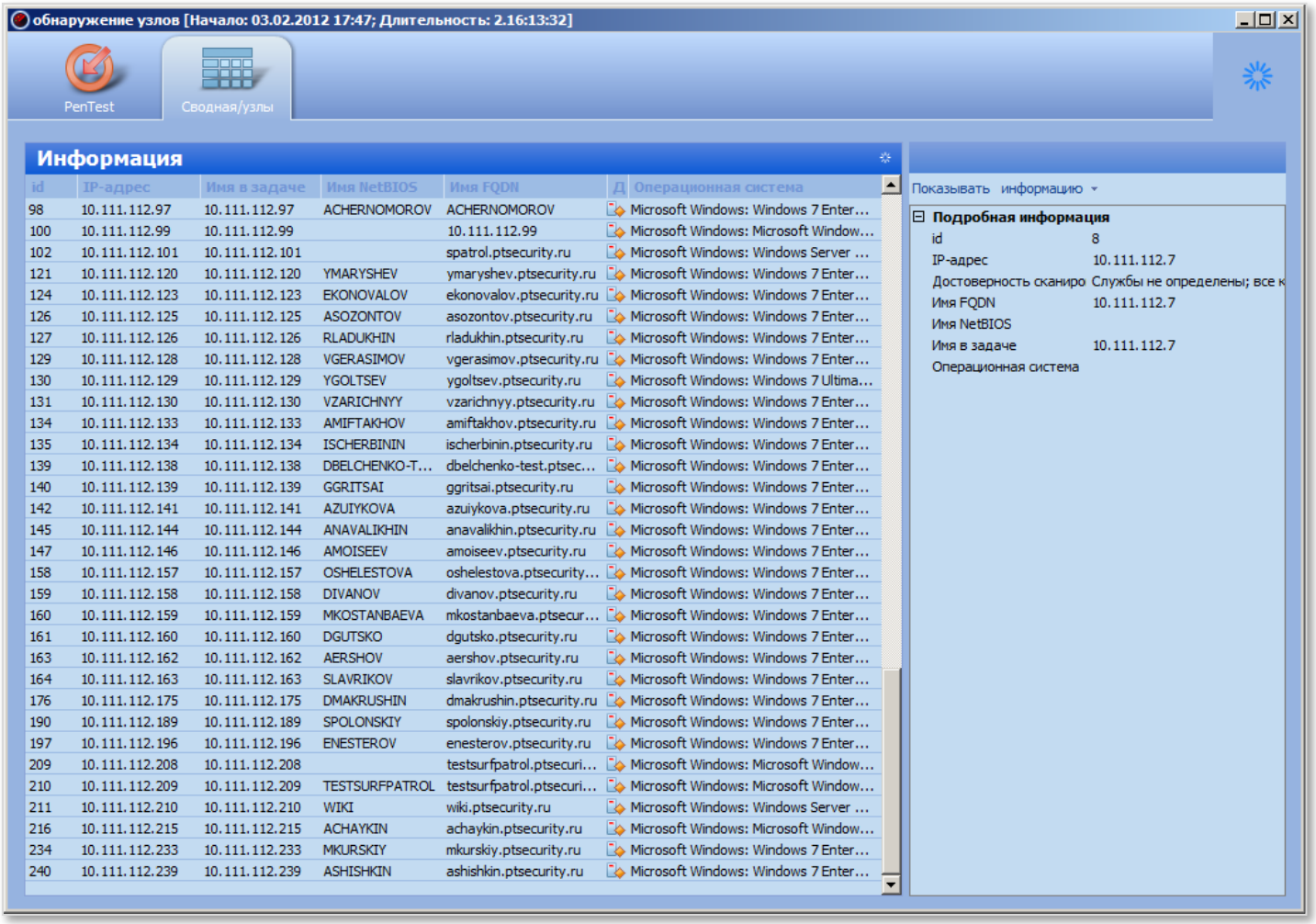
Этапы оценки рисков \ Уровень зрелости	Низкий	Средний	Высокий
Инвентаризация ресурсов	+	+	+
Категорирование ресурсов		±	+
Определение угроз			+
Определение уязвимостей	+	+	+
Определение контрмер	+	+	+

Низкий уровень зрелости

— **Инвентаризация ресурсов:** узлы, ПО
— **Классификация** – только по инфраструктурному признаку:
  – Серверы, ключевые сетевые устройства (критичные)
  – Рабочие станции (некритичные)
— **Определение уязвимостей:** только критичные
— **Определение контрмер:** для критичных и некритичных ресурсов

POSITIVE TECHNOLOGIES

Инвентаризация



Обнаружение ПО

Операционная система

Версия

Windows 7 Enterprise Service Pack 1 (x64)	Метод определения: эвристический

Анализируемое ПО

Название	Версия	Путь
7-Zip	9.20	C:\Program Files\7-Zip
Firefox	8.0.1	
Google Chrome	18.0.1025.168	
IBM Lotus Notes	8.0.1	
Kaspersky Anti-Virus for Windows Workstations	6.0.4.1424	C:\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Workstations MP4
MaxPatrol	8.23.1.12895	C:\Program files\Positive Technologies\MaxPatrol\
Microsoft .NET Framework	2.0 SP2	

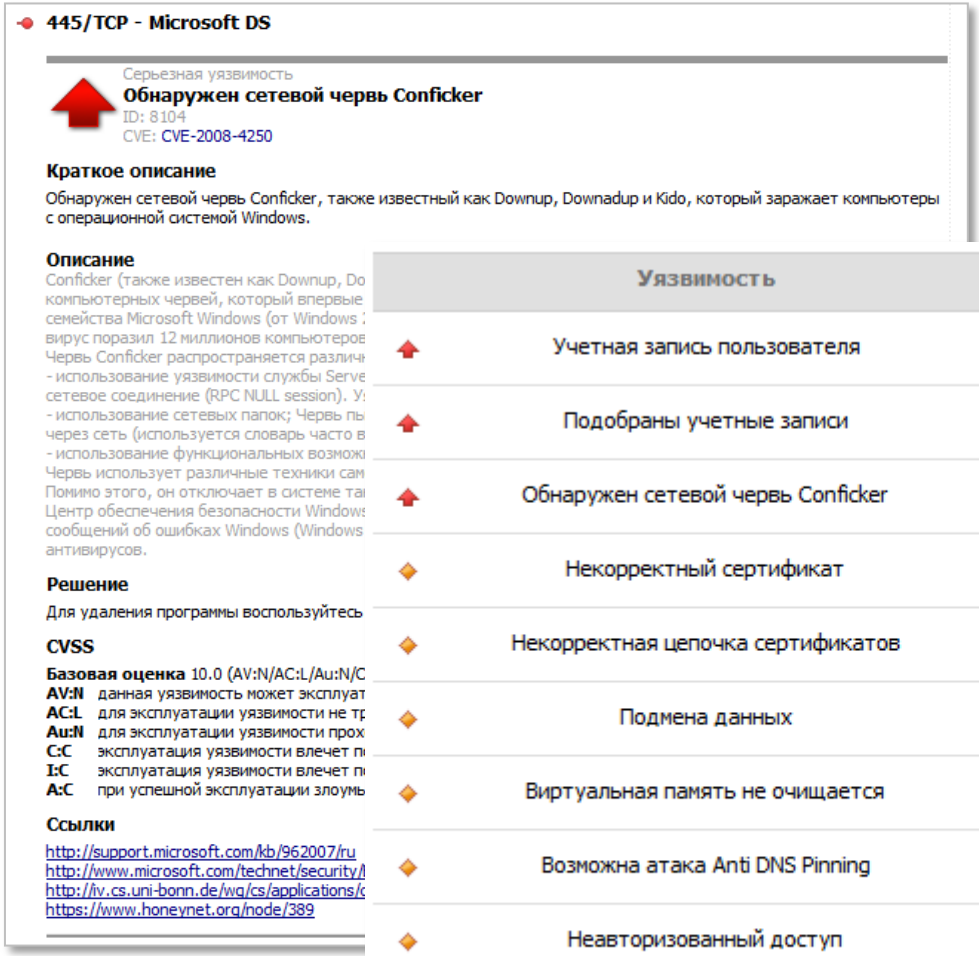
Классификация

Информация

i.	IP-адрес	Имя в задаче	Имя NetBI...	Имя FQDN	Д	Операционная система
3	10.111.115.176	10.111.115.176	WIN7WMI	WIN7WMI		Microsoft Windows: Windows 7 Enterprise Service Pack 1 (x64)
2	10.111.113.197	10.111.113.197		10.111.113.197		Cisco IOS: 12.3(4)T2
4	10.111.115.172	10.111.115.172	DCA2008	DCA2008		Microsoft Windows: Windows 2008 R2 ServerEnterprise Service Pack 1 (x64)
1	10.111.115.175	10.111.115.175	WIN7_MP	WIN7_MP		Microsoft Windows: Windows 7 Enterprise Service Pack 1 (x64)

IP	NETBios	OS	Функция
1.1.1.1	nk	MS Windows 7	рабочая станция
1.1.1.2	es	MS Windows 7	рабочая станция
1.1.1.3	vk	RHEL	сервер
1.1.1.4	sd	RHEL	сервер
1.1.1.5	fg	HP-UX	сервер
1.1.1.6	bn	Cisco IOS	маршрутизатор
1.1.1.7	er	Cisco IOS	маршрутизатор

Обнаружение уязвимостей

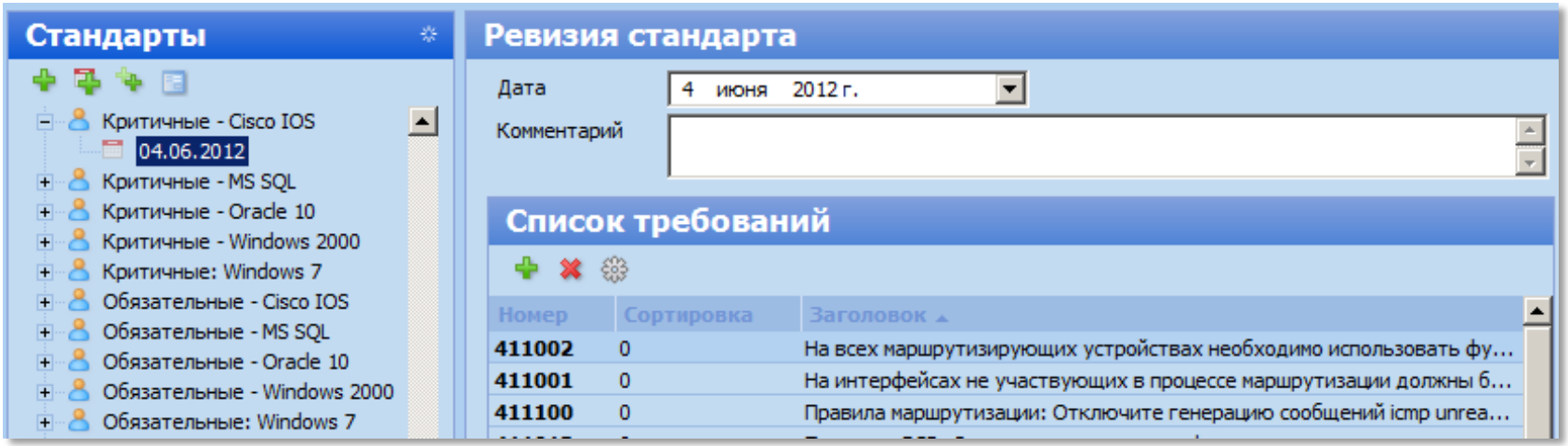


Уязвимость	CVE	Количество
Учетная запись пользователя		5
Подобраны учетные записи		5
Обнаружен сетевой червь Conficker	CVE-2008-4250	2
Некорректный сертификат		6
Некорректная цепочка сертификатов		6
Подмена данных	CVE-2005-1794	5
Виртуальная память не очищается		5
Возможна атака Anti DNS Pinning		2
Неавторизованный доступ	CVE-2009-3555	1
Планировщик заданий		9

Выбор применимых требований

На основе лучших практик и экспертного мнения выбираются наборы требований:

- критичные — для важных инфраструктурных элементов;
- обязательные — для всех остальных.



Результат

— Определены перечень узлов и установленное на них ПО.
— Узлы ранжированы по инфраструктурному признаку.
— Выявлены критичные уязвимости.
— Определены базовые перечни требований для критичных и некритичных ресурсов.

— Необходимо выявить, какие требования не выполняются, — и приступить к их реализации.

Средний уровень зрелости

— **Инвентаризация ресурсов:** узлы, ПО, функции.

— **Классификация** — по инфраструктурному признаку и по принадлежности к бизнес-процессам:

  – критичным:

    • ключевые сетевые устройства;

    • ресурсы БП «Логистика»;

  – некритичным: например, серверы тестовых сред.

— **Определение уязвимостей:** высокая и средняя критичность.

— **Определение контрмер.**

Инвентаризация

IP	NETBios	FQDN	OS	Установленное ПО	БП	Функция
1.1.1.1	nk	nk.company.ru	MS Windows 7	MS Office	Бухгалтерия	рабочая станция
				Google Chrome		
				Касперский		
				…		
1.1.1.2	es	es.company.ru	MS Windows 7	MS Office	Аппарат генерального директора	рабочая станция
				…		

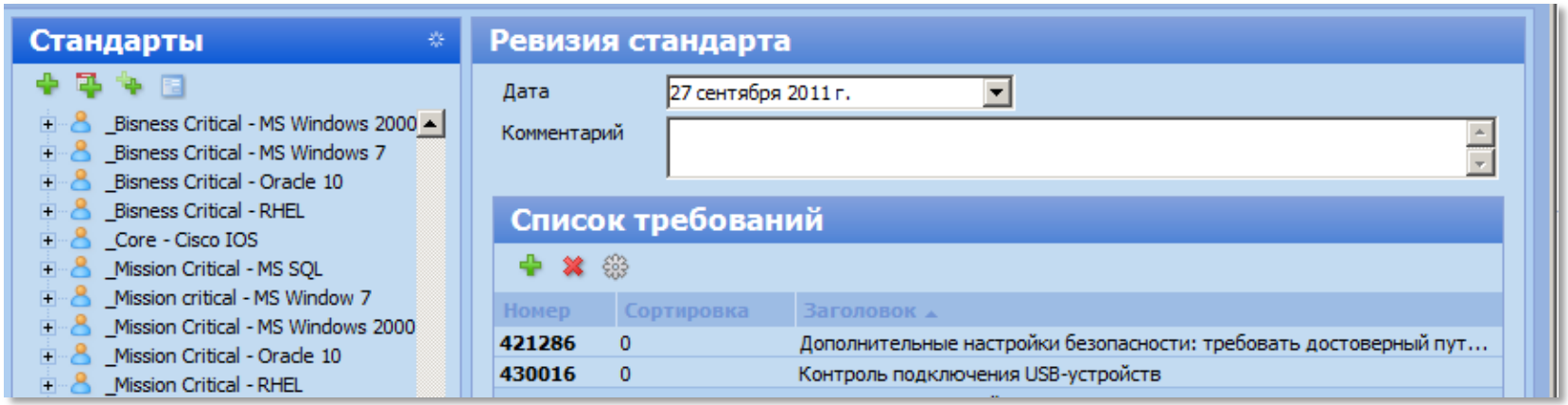
Классификация

Бизнес-процесс	Критичность
Логистика	1 ↑↑
Продажи	1 ↑↑
Производство	1 ↑↑
Склад	1 ↑↑
Аппарат ГД	2 ↑
Бухгалтерия	2 ↑
АХУ	3 ↑

Уровень	Расшифровка
1 ↑↑	Mission Critical
2 ↑	Business Critical
3 ↑	Operations

Выбор применимых требований

— Требования выбираются, исходя из уровня критичность бизнес-приложений, а также принадлежности к ключевой инфраструктуре компании



Результат

— Определены перечень узлов и установленное на них ПО.
— Узлы ранжированы по инфраструктурному признаку, а также по их принадлежности к бизнес-процессам.
— Выявлены уязвимости.
— Определены перечни требований для групп ресурсов.

— Необходимо выявить, какие требования не выполняются, — и приступить к их реализации.

Высокий уровень зрелости

- **Определить риски:**
  - определить активы компании и их владельцев;
  - определить угрозы, действующие на активы;
  - определить уязвимости, которые могут быть реализованы посредством угроз;
  - определить влияние нарушения конфиденциальности, целостности и доступности активов.
- **Проанализировать и оценить риски:**
  - оценить воздействие нарушения безопасности на бизнес-процессы компании;
  - оценить вероятность нарушения безопасности, учитывая доминирующие угрозы и уязвимости;
  - оценить уровень риска;
  - определить, является ли риск приемлемым или требует снижения;
- **Определить и оценить меры по снижению рисков. Возможные меры могут включать:**
  - применение необходимых мер и средств защиты;
  - разумное и объективное принятие рисков;
  - уклонение от рисков;
  - передачу соответствующих рисков третьей стороне.
- **Выбрать цели, меры и средства снижения рисков.**
- **Разработать план снижения рисков.**
- **Установить меры и средства снижения рисков.**

Заключение

— Для любого уровня зрелости компании существуют механизмы *осознанного* определения средств защиты. И это не всегда полноценный анализ рисков.

— Повышение уровня зрелости компании — в наших руках. Успешные методы управления информационной безопасностью неизбежно распространятся на всю компанию.

POSITIVE TECHNOLOGIES

Конец рассказа
Спасибо за внимание

Наталья Куканова

nkukanova@ptsecurity.ru