SPACE·BIT

Выполнение требований регуляторов по управлению безопасностью конфигурирования ПО

Валерий Ледовской
Менеджер по развитию бизнеса Spacebit

Управление уязвимостями в информационных системах

Категория уязвимости	Распространенные методы предотвращения уязвимостей данной категории	В чьей зоне ответственности?
Уязвимости проектирования	▪ Моделирование угроз и нарушителей ▪ Включение требований безопасности в задание на создание системы	Разработчик
Уязвимости реализации	▪ Анализ безопасности исходного кода приложений ▪ Тестирование безопасности при приемке системы ▪ Устранение выявленных уязвимостей уровня реализации	Разработчик
Уязвимости конфигурации	▪ **Разработка и применение стандартов безопасной конфигурации** ▪ **Периодическое тестирование безопасности** ▪ **Периодическое сканирование уязвимостей** ▪ **Установка обновлений безопасности, устраняющих известные уязвимости**	**Потребитель**

82 % уязвимостей связаны с человеческим фактором

Даже при полной автоматизации управления уязвимости необходимо периодически проверять наличие точечных небезопасных изменений конфигурации

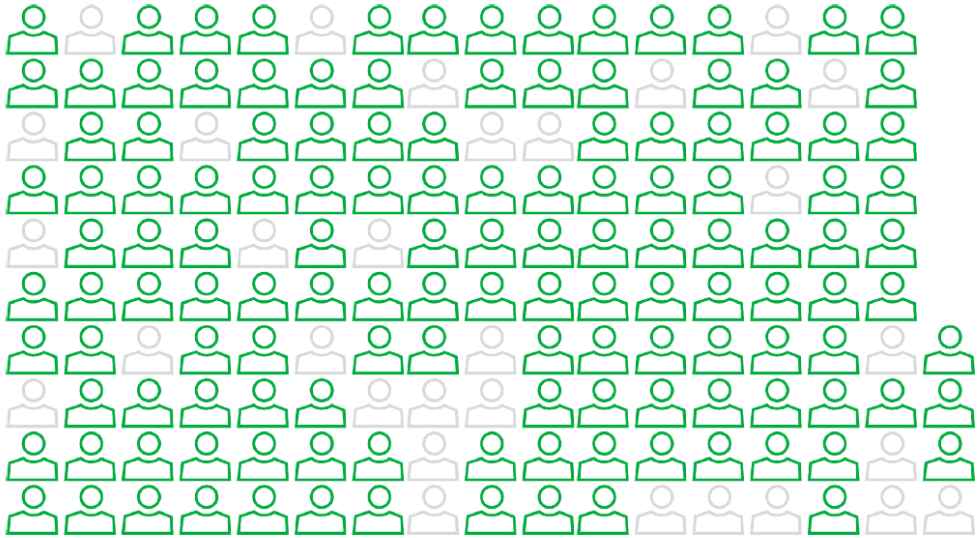


Figure 9. The human element in breaches (n=4,110)
Each glyph represents 25 breaches.

(c) Data Breach Investigations Report, Verizon, 2022

SPACE-BIT

Уязвимости, связанные с ошибками человека

40% ошибок связаны с ошибками при конфигурировании ПО

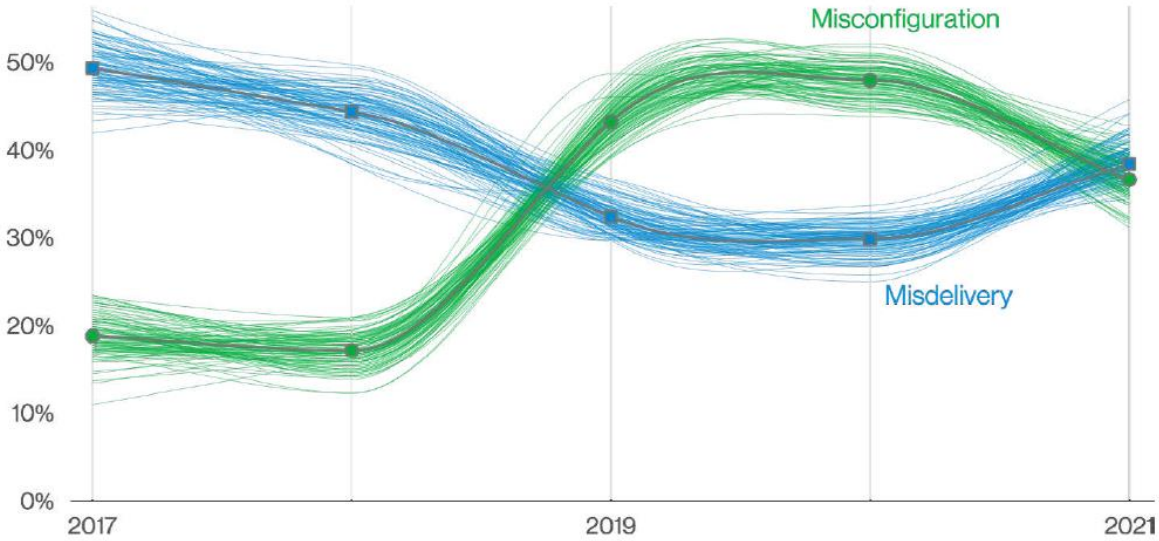
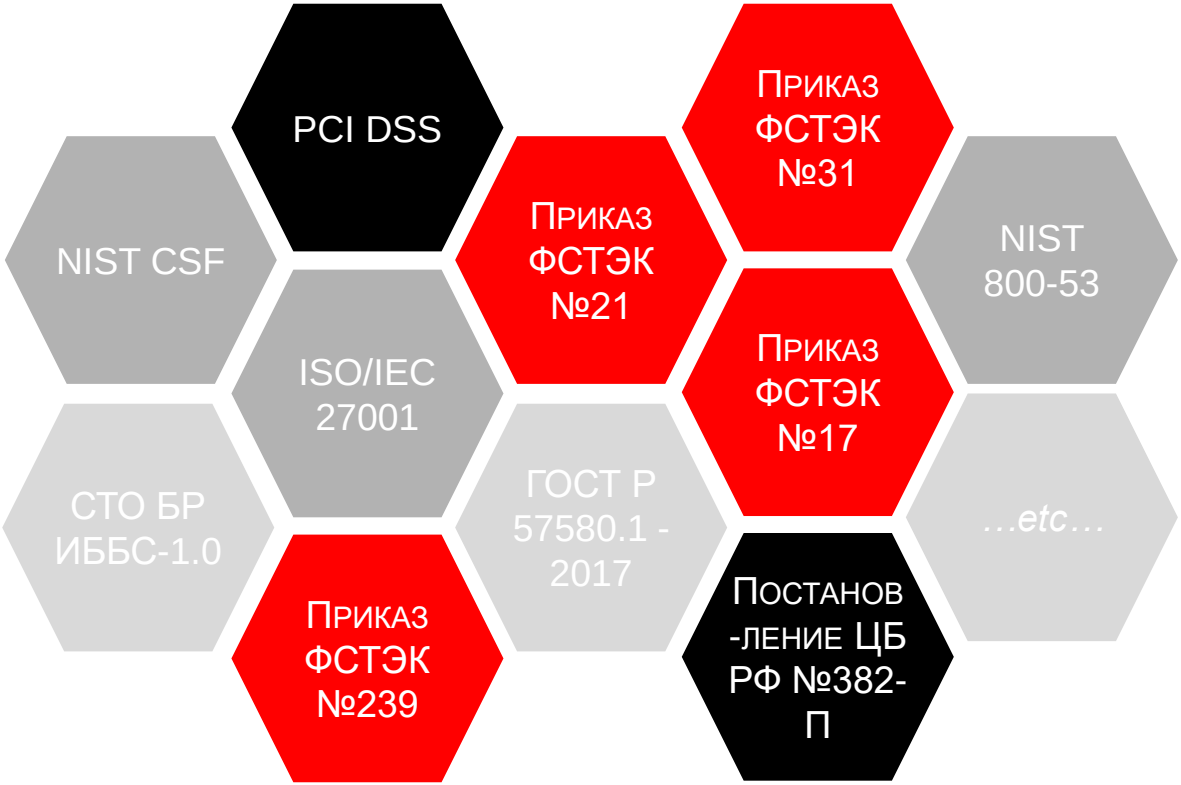


Figure 61. Top Action varieties over time in Miscellaneous Errors breaches

(c) Data Breach Investigations Report, Verizon, 2022

Требования регуляторов к конфигурациям объектов информационной инфраструктуры



В области ИБ существует множество требований регуляторов и отраслевых стандартов. Они определяют требования по управлению уязвимостями, и прежде всего – уязвимостями конфигурации:

- проведение сканирования уязвимостей
- проведение тестов на проникновение
- своевременное устранение уязвимостей
- установка обновлений безопасности
- разработка и применение стандартов безопасной конфигурации

SPACE·BIT

Требования регуляторов

- Сферы: финансовые и страховые организации

Банк России (ГОСТ Р 57580.1-2017)

- Сферы: здравоохранение, наука, транспорт, связь, энергетика, финансовый сектор, топливно-энергетический комплекс, атомная энергетика

КИИ (ФЗ-187)

- Сферы применения: торговые предприятия, финансовые учреждения, разработчики ПО и аппаратного обеспечения для этой области, сервис-провайдеры

PCI-DSS

SPACE-BIT

Источники данных по теме безопасности конфигураций

- **Требования регуляторов** (Банк России, ФСТЭК, платёжные системы);
- **Лучшие практики** (Бенчмарки CIS – Center of Internet Security);
- **Экспертиза** своих сотрудников или внешних специалистов;
- Информация от **производителей ПО**

Как выглядят требования к конфигурациям в бенчмарках?

Бенчмарки по конфигурациям громоздкие и не оцифрованные

1.1 Password Policy

This section contains recommendations for password policy.

1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for Windows Vista is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password.

The recommended state for this setting is: `24 or more password(s)`.

Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another

CIS Microsoft Windows 10 Enterprise Benchmark, v.1.12.0, 15.02.2022, 1278 страниц

SPACE·BIT

Распространенные подходы к управлению конфигурациями не работают

Процедуры управления уязвимостями	?	Определены, но не работают
Разработка и применение стандартов безопасной конфигурации	✗	Мера не применяется
Своевременная установка обновлений безопасности	?	Реализация недостаточно эффективна
Сканирование уязвимостей	?	Реализация недостаточно эффективна
Тестирование на проникновение	✗	Мера не применяется
Устранение выявленных уязвимостей конфигурации	✗	Мера не применяется

SPACE-BIT

Типы программных СЗИ по теме безопасности конфигурации ПО

- Сканеры уязвимостей (VM, Vulnerability Management);
- Базы данных управления конфигурацией (CMDB, мониторинг активов, инвентаризация активов)
- Контроль устройств (MDM, UEM);
- Инструменты для организации **процесса информационной безопасности** по обеспечению безопасных конфигураций ПО

SPACE·BIT

Спасибо за внимание!

Валерий Ледовской
Менеджер по развитию бизнеса Spacebit

www.spacebit.ru

v.ledovskoy@spacebit.ru

+7(905)417-71-12