# Аннотация

Харденинг — это усиление защиты технических и программных средств путем их настройки. Усиление защиты происходит вследствие:

* отключения неиспользуемых функций;
* изменения настроек по умолчанию;
* внесения изменений, повышающих защищенность системы (изменяются права доступа, включаются и настраиваются дополнительные встроенные механизмы защиты).

Таким образом, харденинг обеспечивает защиту технических и программных средств, помогает предотвратить несанкционированный доступ и сбои.

# Какие процессы задействуются при харденинге

Для успешного применения харденинга в организации необходимо обеспечить работу следующих процессов: «Управление конфигурациями», «Управление изменениями», «Управление эксплуатацией», «Управление активами», «Управление выявлением требований»:

* Процесс «Управление конфигурациями» выполняет настройку параметров устройств и отображает актуальную информацию об IT-активах и их связях. Соответственно, именно он позволяет осуществить харденинг оборудования и ПО.
* Процесс «Управление изменениями» обеспечивает проведение согласованных изменений, в том числе применение настроек харденинга или изменение ранее примененных настроек харденинга.
* Процесс «Управление эксплуатацией» непосредственно вносит изменения. Является частью работы специалистов, отвечающих за эксплуатацию (администрирование) технических и программных средств.
* Процесс «Управление активами» разрабатывает инструкции по харденингу: позволяет получить информацию об используемых в организации активах.
* Процесс «Управление выявлением требований» позволяет определять требования, которым должны соответствовать технические и программные средства в организации, отслеживать их и анализировать возможность исполнения.

# Факторы, снижающие эффективность харденинга

Харденинг — это своего рода закручивание гаек и донастройка систем. Следующие факторы могут существенно снизить его эффективность:

* Отсутствие физической защищенности оборудования — если оборудование украдено или повреждено, а информация, хранившаяся на нем, не зашифрована или уничтожена, то харденинг не поможет.
* Несвоевременная установка обновлений — без них оборудование и ПО очень скоро станут уязвимыми.
* Отсутствие периодического резервного копирования — без него невозможно восстановить информацию в случае успешной атаки злоумышленников.
* Отсутствие формализованного механизма внесения изменений в конфигурацию оборудования и ПО (в том числе в целях харденинга) — это не позволит управлять конфигурацией и контролировать ее.

# Алгоритм разработки инструкции по харденингу

Прежде чем начать разрабатывать инструкцию по харденингу, рекомендуется найти готовые руководства и инструменты, оценить их применимость для системы или в перечне источников инструкций и инструментов. При разработке собственной инструкции рекомендуется следовать следующему алгоритму:

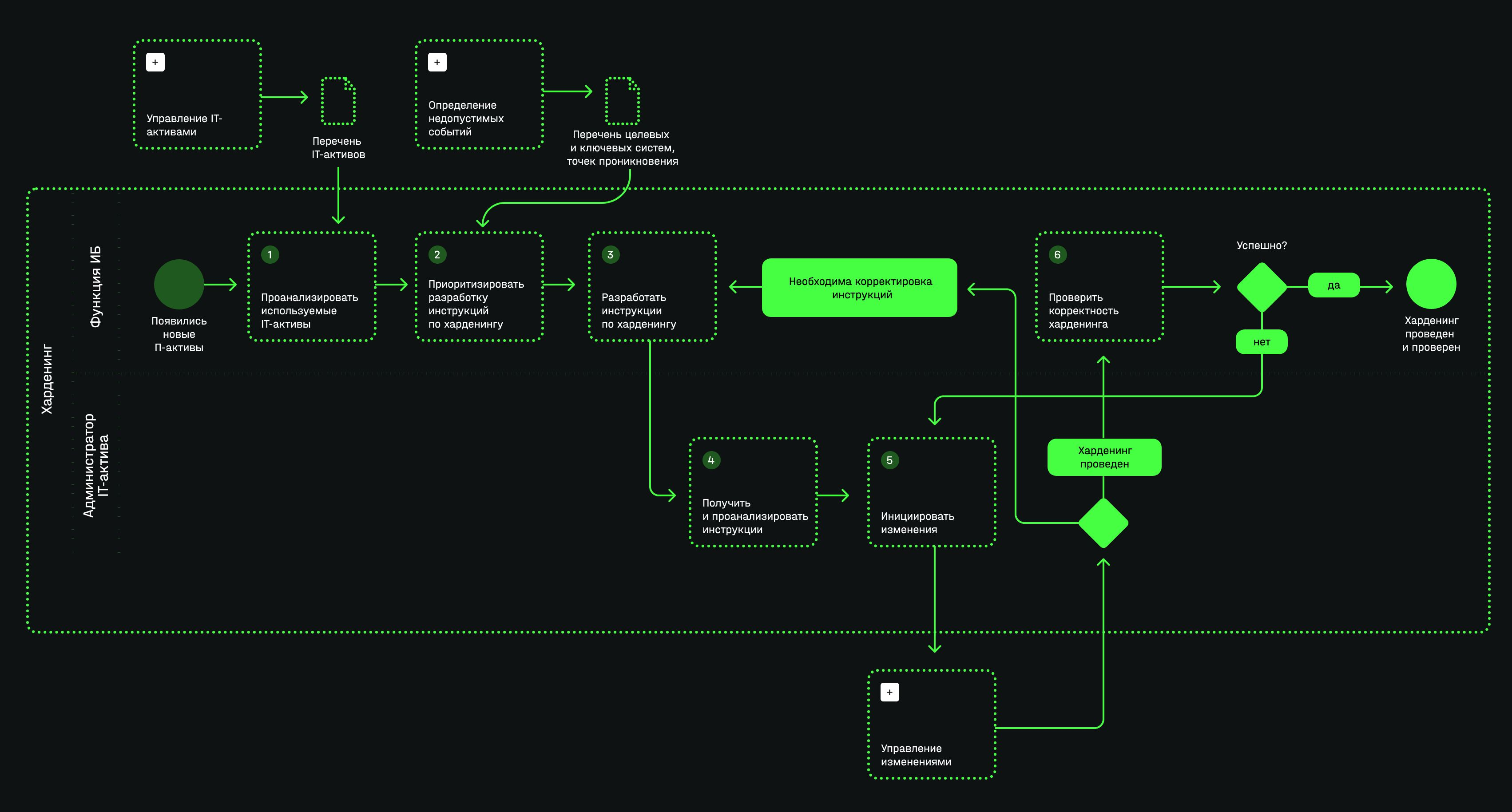
1. Определить назначение объекта харденинга (ОС, СУБД, встроенное ПО, прикладное ПО и прочее).
2. Выявить сетевые взаимодействия и взаимодействия с другими компонентами внутри операционной системы в рамках осуществляемых функций объекта харденинга.
3. Отключить все неиспользуемые функции объекта харденинга (пакеты, модули и т. п.).
4. Отключить все учетные записи, используемые по умолчанию, или сменить пароли, установленные по умолчанию (при наличии).
5. Проанализировать параметры объекта, доступные для изменения, и их влияние на защищенность и функциональность.
6. Определить значения настроек, обеспечивающих или усиливающих защищенность объекта харденинга.
7. Протестировать инструкцию на тестовом стенде.

Каждая система может состоять из множества объектов харденинга, которые будут отличаться в зависимости от роли системы (например, проект, СЗИ или сервер контроллера домена).

# Описание процесса харденинга

Обобщенная схема процесса харденинга приведена на рисунке.

| **Шаг** | **Описание шага** |
| --- | --- |
| Шаг 1. Проанализировать используемые IT-активы | Функция ИБ должна определить все IT-активы, существующие в организации, а также выявить, для каких из них уже имеются инструкции по харденингу, а для каких нет |
| Шаг 2. Приоритизировать разработку инструкций по харденингу | Выбор объекта для харденинга начинается с приоритизации защищаемых информационных ресурсов. Из всех IT-активов, к которым нет инструкций, нужно выбрать наиболее ценные и подверженные атакам. Если предварительно были выявлены точки проникновения во внутреннюю сеть организации, то в большинстве случаев именно с них и следует начинать харденинг: они являются первой целью злоумышленников. Далее в качестве объектов следует рассматривать целевые и ключевые системы |
| Шаг 3. Разработать инструкции по харденингу | Необходимо разработать инструкцию по харденингу IT-актива согласно алгоритму, приведенному в разделе «Алгоритм разработки инструкции по харденингу» |
| Шаг 4. Получить и проанализировать инструкции | Владелец IT-актива (лицо, ответственное за техническое администрирование) анализирует поступившую инструкцию, определяя число активов, к которым необходимо применить изменения, и объем работы |
| Шаг 5. Инициировать изменение | Владелец IT-актива инициирует харденинг в рамках процесса управления изменениями, установленного в организации |
| Шаг 6. Проверить корректность харденинга | Функция ИБ проверяет корректность произведенного харденинга |



*Рисунок 1. Обобщенная схема процесса харденинга*

# Применение инструкции по харденингу систем

После успешной разработки и применения инструкции к приоритизированным активам встает вопрос о ее распространении на другие активы. Для распространения используются «золотые» образы — преднастроенные системы, готовые для развертывания. Таким образом, в организации должен быть сформирован пул «золотых» образов систем. Изменения, вносимые в них, согласовываются с функцией ИБ.

# Обновление инструкции по харденингу

Триггерами к пересмотру инструкции могут быть:

* Обновление версии программного продукта. Необходимо проанализировать изменения функциональности и их влияние на инструкцию по харденингу. Если выявлены серьезные изменения, следует пересмотреть инструкцию.
* Неэффективность имеющейся инструкции (может быть выявлена, например, по результатам верификации недопустимых событий или в ходе тестирования изменения).
* Неработоспособность системы после применения инструкции по харденингу (выявляется на этапе тестирования изменения).

# Приложение 1

Ссылка инструментами по проверке безопасности ОС:

<https://github.com/vit81g/awesome-security-hardening?tab=readme-ov-file#hardening-guide-collections>