Аннотация – документ "Choosing Secure and Verifiable Technologies" содержит анализ основных аспектов выбора защищённых цифровых продуктов и услуг и охватывает различные области, включая принципы безопасности при проектировании, прозрачность производителя, управление рисками, риски цепочки поставок и рекомендации после покупки, такие как политика технического обслуживания и окончания срока службы. Каждый раздел предлагает подробное изучение стратегий и практик, повышающих безопасность и достоверность технологических закупок.

Этот документ особенно полезен специалистам по кибербезопасности, ИТ-менеджерам и специалистам по закупкам в различных отраслях. Он служит ценным ресурсом, поскольку в нем описываются необходимые шаги для обеспечения того, чтобы приобретённые технологии не только соответствовали текущим стандартам безопасности, но и соответствовали текущим методам обеспечения безопасности для уменьшения будущих уязвимостей. Этот анализ направлен на принятие обоснованных решений, защищающих данные организации и инфраструктуру от потенциальных киберугроз, тем самым повышая общую устойчивость бизнеса. Интегрируя эти методы, специалисты из различных секторов могут значительно снизить риски, связанные с цифровыми технологиями, и повысить безопасность их эксплуатации.

I. Введение

Документ “Choosing Secure and Verifiable Technologies” содержит всеобъемлющее руководство для организаций по приобретению цифровых продуктов и услуг с акцентом на безопасность, начиная с этапа проектирования и заканчивая жизненным циклом технологии.

В документе подчёркивается критическая важность выбора технологий, которые по своей сути являются безопасными, для защиты конфиденциальности пользователей и данных от растущего числа киберугроз. В нем излагается ответственность клиентов за оценку безопасности, пригодности и связанных с ними рисков цифровых продуктов и услуг. ИТ-отдел выступает за переход к продуктам и услугам, которые безопасны как с точки зрения проектирования, так и по умолчанию, подчёркивая преимущества такого подхода, включая повышение устойчивости, снижение рисков и снижение затрат, связанных с исправлениями и реагированием на инциденты.

- **Безопасность по умолчанию**: необходимость проектирования и разработки технологий, обеспечивающих безопасность, является основополагающим элементом безопасности продуктов при минимальной потребности в дополнительных конфигурациях.
- **Процесс закупок**: двухэтапный подход к закупкам – оценка перед включает оценку функций безопасности продукта, прозрачности производителя и постоянной поддержки и обновлений, предоставляемых производителем.
- **Прозрачность производителя**: Организациям рекомендуется оценить приверженность производителя обеспечению безопасности, включая его способность предоставлять информацию о функциях безопасности и уязвимостях продукта. Производители должны придерживаться такой практики, как публикация полных и своевременных материалов.
- **Управление рисками**: важность непрерывного управления рисками как в процессе закупок, так и на протяжении всего жизненного цикла продукта или услуги включает регулярные обновления и исправления от производителя для устранения новых уязвимостей.
- **Риски цепочки поставок:** здесь основное внимание уделяется управлению рисками, связанными с цепочкой поставок, при этом подчёркивается необходимость того, чтобы организации обеспечивали соблюдение их поставщиками проектных принципов безопасности.
- **Управление инцидентами безопасности**: охватывает необходимость эффективного управления инцидентами безопасности и событиями (SIEM) и интеграции управления безопасностью, автоматизации и реагирования (SOAR) для управления потенциальными инцидентами безопасности и смягчения их последствий.
- **Политика жизненного цикла**: необходимость чёткой политики в отношении срока службы продуктов и услуг, включая безопасное удаление данных и переход на новые технологии.
- **Вопросы регулирования и соответствия**: организациям рекомендуется обеспечивать соответствие продуктов и услуг требованиям и стандартам, которые могут варьироваться в зависимости от отрасли и типа обрабатываемых данных.

II. Аудитория

Документ ориентирован на широкую аудиторию в сфере закупок и производства цифровых технологий.:

- **Организации, которые закупают и используют цифровые продукты и услуги**: широкий круг организаций, известных как закупающие организации, закупщики, потребители и заказчики. Эти организации находятся в центре внимания руководства документа, направленного на совершенствование процесса принятия ими решений при закупке цифровых технологий.
- **Производители цифровых продуктов и услуг**: Документ также адресован производителям цифровых технологий, предоставляя им информацию о принципах обеспечения безопасности при разработке. Это предназначено для руководства производителями при разработке технологий, отвечающих ожиданиям их клиентов в области безопасности.

Ключевым сотрудникам, которым рекомендуется ознакомиться с данным руководством и использовать его:

- **Руководители организаций и менеджеры высшего звена**: играют решающую роль в принятии решений и формулировании стратегии для своих организаций.
- **Персонал по кибербезопасности и политике безопасности**: ответственные за обеспечение безопасности цифровых технологий в своих организациях.
- **Команды разработчиков продуктов**: участвуют в создании и разработке цифровых продуктов и услуг, обеспечивая безопасность этих предложений по своей конструкции.
- **Консультанты по рискам и специалисты по закупкам**: консультируют по вопросам управления рисками и специализируются на процессе закупок, гарантируя, что приобретаемые цифровые технологии не представляют неоправданных рисков для организации.

Документ преследует несколько целей:

- Информировать организации о проектных принципах безопасности при приобретении цифровых продуктов и услуг, что приводит к более обоснованным оценкам и решениям.
- Информировать производителей о конструктивных принципах безопасности их продуктов и услуг с целью ускорения разработки безопасных технологий. Это даёт производителям ответы на ключевые вопросы безопасности и ожидания, которые они могут ожидать от своих клиентов.

В документе подчёркивается, что это не контрольный список для получения идеальных результатов цифровых закупок, а скорее руководство, помогающее закупающим организациям принимать обоснованные решения с учётом рисков в их уникальных операционных контекстах. Признается уникальность структуры и подхода каждой организации к закупкам и предполагается, что не каждый пункт документа может иметь отношение к каждой организации. Кроме того, организациям может потребоваться учитывать другие факторы, не описанные в документе, которые могут быть уникальными для их конкретной ситуации или отрасли или региона, в котором они работают.

III. Концепция “Security by design”

Концепция "Security by design" (SbD) — это упреждающий подход, ориентированный на безопасность, применяемый производителями программного обеспечения при разработке цифровых продуктов и услуг. Такой подход требует целенаправленного согласования целей кибербезопасности на всех организационных уровнях, задействованных в производственном процессе.

- **Проактивная интеграция безопасности**: подход требует, чтобы принципы были интегрированы с самого начала процесса разработки продукта, а не добавлялись как запоздалая мысль. Такая интеграция происходит на всех этапах проектирования, разработки и развёртывания.
- **Целенаправленное согласование целей в области кибербезопасности**: подход требует, чтобы цели кибербезопасности согласовывались с самого начала с бизнес-целями и дизайном продукта. Такое согласование гарантирует, что меры безопасности встроены в архитектуру продукта или услуги.
- **Учёт киберугроз**: Производители должны учитывать потенциальные киберугрозы на начальных этапах разработки продукта. Такое прогнозирование позволяет реализовать меры по смягчению последствий на ранних стадиях процесса разработки, снижая вероятность появления уязвимостей в конечном продукте.
- **Конфиденциальность пользователей и защиты данных**: Основной целью подхода является конфиденциальности пользователей и защита данных. Разрабатывая продукты с меньшим количеством уязвимостей, производители повышают безопасность пользовательских данных от несанкционированного доступа и потенциальных утечек.
- **Руководство для закупающих организаций**: Понимание принципов подхода имеет решающее значение для организаций, закупающих цифровые продукты и услуги. Эти знания помогают им принимать обоснованные решения, гарантируя, что приобретаемые ими продукты построены с учётом безопасности в качестве основополагающего элемента

IV. Изменение баланса рисков кибербезопасности

Рассматриваемый документ ссылается на другой “Choosing Secure and Verifiable Technologies” от Агентства по кибербезопасности и инфраструктурной безопасности (CISA), и представляет собой совместную работу,

направленную на руководство производителями технологий в повышении безопасности их продуктов. Эта публикация представляет собой международную попытку уменьшить уязвимости, которые могут быть использованы в технологиях, используемых как государственными, так и частными организациями. Документ поддерживается коалицией агентств глобальной безопасности, включая CISA, Федеральное бюро расследований (ФБР), Агентство национальной безопасности (АНБ) и международных партнёров из Австралии, Канады, Новой Зеландии, Соединённого Королевства, Германии и Нидерландов.

A. *Основополагающие принципы*

- **Ответственность за результаты обеспечения безопасности клиентов**: производителям рекомендуется уделять приоритетное внимание безопасности своих клиентов, интегрируя принципы безопасности с начальных этапов разработки продукта. Этот принцип подчёркивает важность разработки продуктов, которые по своей сути являются безопасными, тем самым снижая риск киберугроз для конечных пользователей.
- **Радикальная прозрачность и подотчётность**: принцип призывает производителей быть открытыми и прозрачными в отношении функций безопасности своей продукции. Он призывает раскрывать потенциальные уязвимости и шаги, предпринятые для их устранения, способствуя формированию культуры подотчётности.
- **Безопасность — это бизнес-цель**: В техническом документе подчёркивается важнейшая роль руководителей высшего звена во внедрении безопасности в корпоративную культуру. Это предполагает, что руководство должно отстаивать безопасность как основную бизнес-цель, гарантируя, что она будет считаться приоритетной на протяжении всего жизненного цикла разработки продукта.

B. *Воздействие и реализация*

Документ предоставляет производителям план разработки продуктов, безопасных с точки зрения проектирования и по умолчанию, обеспечивающих защиту от распространённых киберугроз без необходимости дополнительных настроек или затрат для конечных пользователей. Это предполагает, что принятие этих принципов может переложить бремя обеспечения безопасности с потребителей на производителей, снижая вероятность инцидентов безопасности, возникающих в результате распространённых проблем, таких как неправильная конфигурация или задержка с исправлением.

Кроме того, в документе подчёркивается необходимость стратегического внимания к безопасности программного обеспечения, призывая производителей идти на сложные компромиссы и инвестиции, включая внедрение языков программирования, которые смягчают распространённые уязвимости, и отдавать приоритет безопасности, а не привлекательным, но потенциально рискованным функциональным возможностям их продуктов.

V. Категории цифровых продуктов и услуг

Различные категории цифровых продуктов и услуг подчёркивают важность понимания этих категорий для обеспечения безопасной закупки и использования.

A. *Программное обеспечение*

- **Определение**: Программное обеспечение охватывает все типы программ и прикладных программ, включая операционные системы и встроенные системы.
- **Проприетарное программное обеспечение**: это программное обеспечение, разработанное производителями и распространяемое по специальным соглашениям о лицензировании или покупке. Он часто имеет ограничения, такие как ограничения пользователей и запреты на перепродажу или модификацию.
- **Программное обеспечение с открытым исходным кодом (OSS)**: OSS включает программное обеспечение с исходным кодом, которое находится в свободном доступе по открытой лицензии, позволяющей любому просматривать, использовать, изучать или изменять его. Управляемая сообществом волонтёров, OSS способствует быстрой разработке продукта благодаря своему характеру сотрудничества.

B. *Встроенное программное обеспечение и микропрограммное обеспечение*

- **Встроенное программное обеспечение**: это программное обеспечение управляет встроенными системами, предназначенными для выполнения определённых функций в рамках более крупных систем, обычно ограниченных доступными вычислительными ресурсами и предназначенных для операций в режиме реального времени.
- **Прошивка**: Тип встроенного программного обеспечения, прошивка постоянно хранится в энергонезависимой памяти устройства и обеспечивает низкоуровневый контроль над аппаратными компонентами устройства.

C. *Спецификация программного обеспечения (SBOM)*

- **Функциональность**: SBOM содержит список программных компонентов или библиотек, составляющих программный пакет. Это применимо ко всем типам программного обеспечения, включая проприетарное, операционное, встроенное и прошивное.
- **Полезность**: Спецификации SBOM помогают производителям и потребителям идентифицировать компоненты и их версии в продукте, облегчая мониторинг обновлений и уязвимостей. Спецификации SBOM обычно являются машиночитаемыми для поддержки автоматического мониторинга и отчётности.

D. *Аппаратное обеспечение*

- **Область применения**: Аппаратное обеспечение включает любое физическое устройство,

предназначенное для обработки, хранения или передачи данных. К этой категории относятся сетевые устройства (например, брандмауэры, маршрутизаторы), устройства хранения данных и серверы.

- **Спецификация оборудования (HBOM)**: HBOM описывает физические компоненты, из которых состоит аппаратное устройство. Это крайне важно для понимания материалов, используемых в оборудовании, и оценки потенциальных рисков цепочки поставок.

E. Интернет вещей (IoT)

IoT обычно относится к аппаратному обеспечению и включает устройства и датчики, которые подключаются к Интернету для обмена данными и обеспечения функциональности. В эту категорию входят потребительские товары, медицинские устройства и операционные технологии.

F. Облачные сервисы

Поставщики облачных услуг предлагают вычислительные ресурсы по запросу, включая инфраструктуру, платформу, хранилище, сетевые услуги и обработку данных. Здесь применяются принципы безопасности, аналогичные при закупке программного обеспечения и оборудования.

G. Программное обеспечение как услуга (SaaS)

SaaS позволяет потребителям использовать программное обеспечение без необходимости устанавливать его самостоятельно или управлять им. Это снижает накладные расходы на управление и инфраструктуру и может предлагаться по различным соглашениям, включая бесплатный доступ.

H. Поставщики управляемых услуг (MSP)

MSP предоставляют специализированные услуги, помогающие организациям управлять облачной инфраструктурой, обеспечивать её безопасность и оптимизировать. Услуги включают управление облачной инфраструктурой, безопасность, резервное копирование и восстановление данных, что позволяет клиентам сосредоточиться на основных видах деятельности

VI. Внешние закупки

Внешние закупки подразделяются на этапы перед покупкой и после покупки для обеспечения безопасных и обоснованных решений при приобретении цифровых продуктов и услуг.

A. Этап пред-покупки

Этап фокусируется на нескольких ключевых областях для обеспечения того, чтобы организации делали осознанный и безопасный выбор при приобретении цифровых продуктов и услуг.

1) Прозрачность и отчётность

- Организациям следует проверять прозрачность информации, предоставляемой производителями, которая может включать отраслевые отчёты, независимое тестирование и обновления функций безопасности.
- Ожидается, что производители будут уведомлять клиентов о любых обнаруженных уязвимостях и предоставлять рекомендации по их устранению, в идеале без каких-либо дополнительных затрат.
- Публикация полных и своевременных отчётов об общих уязвимостях и разоблачениях (CVE) имеет решающее значение для поддержания прозрачности.

2) Защищенный по умолчанию

- Продукты должны быть безопасными "из коробки", требуя от потребителя минимальной настройки системы безопасности для безопасной эксплуатации.
- Функции защиты по умолчанию могут включать многофакторную аутентификацию и ведение журнала безопасности с настройками по умолчанию, настроенными на самый высокий уровень безопасности.

3) Требования безопасности

- Организации должны определять и понимать свои конкретные потребности в области безопасности, чтобы гарантировать соответствие закупаемых продуктов этим требованиям.
- Использование стандартов шифрования и управление идентификационными данными.

4) Управление рисками в цепочке поставок

- Оценка безопасности цепочки поставок производителя имеет жизненно важное значение, поскольку уязвимости могут быть унаследованы закупающей организацией.
- У производителей должен быть план управления рисками в цепочке поставок для устранения потенциальных рисков.

5) Использование программного обеспечения с открытым исходным кодом

- Следует тщательно контролировать использование программного обеспечения с открытым исходным кодом (OSS), чтобы избежать рисков для безопасности.
- Производителям следует обеспечивать регулярное обновление компонентов OSS и их безопасность.

6) Обмен данными и суверенитет

- Понимание того, какие данные будут переданы, как они будут использоваться производителем, и обеспечение соблюдения законов о защите данных имеют решающее значение.
- Учитывается географическое расположение, в котором хранятся и обрабатываются данные.

7) Процесс разработки

- Организациям следует убедиться в том, что производители придерживаются безопасных методов разработки.

- Учитывается, разрабатываются ли продукты в безопасной среде и соответствуют ли они соответствующим стандартам.

8) Геополитические риски

- Производители должны осознавать геополитические риски, которые могут повлиять на их продукцию и услуги, и управлять ими.
- Учитывается понимание политической стабильности регионов, где они работают, и их цепочек поставок.

9) Регулируемые Отрасли

Продукты должны оцениваться на соответствие конкретным нормативным требованиям, относящимся к отрасли, в которой они используются.

10) Доступ к производителю

- Оценка необходимости и безопасности доступа любого производителя к системам организации.
- Учитывается как удалённый, так и физический контроль доступа.

11) Внутренняя угроза

- Учёт потенциальных рисков, исходящие от инсайдеров в организации производителя, которые могут нанести вред закупающей организации.
- Должны быть внедрены такие средства контроля, как надёжная практика найма и мониторинг.

12) Открытые стандарты

- Использование открытых стандартов способствует интероперабельности и снижает риск привязки к поставщику.
- Организациям следует проверять соответствие продукции этим стандартам.

13) Подключенные системы

Понимание всех систем, к которым будет подключаться продукт, важно для оценки потенциальных рисков и эффективного управления ими.

14) Ценность продукта

Оценка ценности продукта, включая его стоимость, ожидаемый срок службы и уровень безопасности, который он обеспечивает организации, имеет решающее значение для принятия обоснованных решений о закупках

B. Этап после покупки

На этапе рассматриваются несколько важнейших аспектов управления цифровыми продуктами и услугами после приобретения. Эти аспекты имеют решающее значение для обеспечения постоянной безопасности, соответствия требованиям и операционной эффективности.

1) Управление рисками

- Организации должны обеспечивать непрерывное управление рисками для устранения новых и эволюционирующих угроз.
- Регулярные оценки и обновления необходимы для адаптации к изменениям в ландшафте угроз и поддержания целостности безопасности технологии на протяжении всего её жизненного цикла.
- Управление инцидентами безопасности, организация безопасности, автоматизация и реагирование на них (SIEM и SOAR)
- Интеграция решений SIEM и SOAR жизненно важна для эффективного обнаружения и устранения вредоносных действий.
- Для оптимальной работы этим инструментам требуются подробные журналы из приложений, и производителям следует сотрудничать с поставщиками SIEM и SOAR, чтобы убедиться, что их продукты регистрируют достаточный объём информации.

2) Техническое обслуживание

- Организации должны проверять соблюдение производителями обязательств по техническому обслуживанию, заявленных на этапе закупок.
- Это включает предоставление своевременных обновлений и исправлений, а также поддержку для устранения любых уязвимостей, обнаруженных после покупки.

3) Контракты, лицензирование и Соглашения об уровне обслуживания

- Важно обеспечить соблюдение производителем всех договорных обязательств и соглашений об уровне обслуживания.
- Организациям следует регулярно проверять эти соглашения, чтобы подтвердить текущее соответствие и учесть любые изменения, которые влияют на качество обслуживания и безопасность.

4) Направляющие для ослабления

- Производители должны предоставлять руководства с подробным описанием параметров конфигурации, которые пользователи могут изменять в продукте.
- В этих руководствах должны быть объяснены последствия для безопасности изменения конфигураций по сравнению с настройками по умолчанию и предложены возможные компенсирующие меры безопасности.

5) Конец жизненного цикла

- Процессом окончания срока службы продукта следует управлять осторожно, чтобы избежать рисков безопасности, связанных с неподдерживаемыми или устаревшими технологиями.
- Организациям следует планировать безопасную утилизацию или передачу продукта в конце срока его службы, гарантируя, что все данные будут надлежащим образом обрабатываться и что продукт будет выведен из эксплуатации способом, обеспечивающим безопасность

VII. Внутренние закупки

Внутренние закупки подразделяются на три этапа: перед закупкой, закупка и после закупки. На каждом этапе рассматриваются конкретные аспекты, которые организациям необходимо учитывать внутри компании при закупке цифровых продуктов и услуг.

A. *Этап пред-покупки*

Этап направлен на обеспечение соответствия внутренних аспектов организации закупкам цифровых продуктов и услуг. Этот этап включает консультации и оценки в различных отделах организации, чтобы убедиться в том, что рассматриваемый продукт или услуга соответствует организационным потребностям и стандартам безопасности.

1) Высшее руководство

- **Оценка и утверждение рисков**: Высшее руководство несёт ответственность за установление порогового значения организационного риска и утверждение закупок на основе комплексной оценки рисков. Это включает в себя понимание потенциальных рисков, связанных с продуктом или услугой, и обеспечение того, чтобы они находились в приемлемых пределах.

- **Включение плана реагирования на инциденты**: для высшего руководства крайне важно обеспечить включение продукта или услуги в план реагирования на инциденты организации, что указывает на готовность к потенциальным инцидентам безопасности.

2) Политика

- **Соответствие политике**: Закупки должны оцениваться в соответствии с существующими политиками, чтобы убедиться в отсутствии конфликтов. Это включает проверку того, что уровень риска, связанный с продуктом или услугой, не превышает принятые организацией пороговые значения риска.

- **Соответствие нормативным и законодательным требованиям**: Продукт или услуга должны соответствовать всем соответствующим требованиям к регистрации и аудиту, которые могут быть продиктованы законодательными или регулирующими стандартами. Это обеспечивает соответствие требованиям и способствует плавной интеграции продукта или услуги в деятельность организации.

3) Инфраструктура и безопасность

- **Совместимость средств контроля безопасности**: Существующие средства контроля безопасности, структуры или стандарты, которых придерживается организация, должны быть совместимы с новым продуктом или услугой. Для оценки этой совместимости следует завершить оценку воздействия на безопасность.

- **Моделирование угроз**: следует разработать тщательную модель угроз для выявления соответствующих угроз и рисков, гарантируя, что управление ими осуществляется на приемлемом уровне. Это помогает понять, как продукт или услуга впишутся в существующую инфраструктуру и какие корректировки могут потребоваться.

4) Владелец продукта

- **Потребности бизнеса и толерантность к риску**: Владелец продукта должен оценить, соответствует ли продукт потребностям бизнеса, не превышая толерантность организации к риску. Это включает в себя оценку уровня секретности, которому должна соответствовать покупка.

- **Контракт и снижение рисков**: контракт должен охватывать приемлемый уровень риска и включать соответствующие меры по снижению рисков. Владелец продукта играет решающую роль в обеспечении соответствия условий контракта и разработке плана снижения рисков

B. *Этап покупки*

Этап включает критические оценки и решения, которые обеспечивают соответствие процесса закупок целям организации и требованиям безопасности.

1) Высшее руководство

- **Принятие решений и принятие рисков**: Высшее руководство несёт ответственность за окончательную доработку решений о закупках. Это включает принятие любых остаточных рисков, выявленных в процессе закупок, и обеспечение того, чтобы эти риски находились в пределах допустимого риска организации.

- **Утверждение контрактов**: Высшее руководство играет решающую роль в рассмотрении и утверждении окончательных контрактов, гарантируя, что все условия соответствуют требованиям организации и что контракты обеспечивают надлежащую защиту и ценность.

2) Системное администрирование

- **Проверка технических спецификаций**: Системным администраторам поручено проверять, соответствуют ли технические спецификации закупаемых продуктов или услуг требованиям организации. Это включает в себя подтверждение правильности реализации всех системных конфигураций, интеграций и пользовательских настроек.

- **Проверки безопасности и соответствия требованиям**: они гарантируют соответствие новых систем существующим политикам и стандартам безопасности. Системные администраторы также играют определённую роль в настройке новых систем для поддержания безопасности и операционной эффективности.

3) Инфраструктура и безопасность

- **Интеграция и совместимость**: основное внимание уделяется обеспечению того, чтобы новые системы закупок беспрепятственно интегрировались с существующей инфраструктурой без ущерба для безопасности или производительности. Это

включает в себя проведение детальных проверок совместимости и планирование любых необходимых обновлений инфраструктуры.

- **Текущие оценки безопасности**: после интеграции крайне важно постоянно оценивать состояние безопасности интегрированных систем для оперативного выявления любых возникающих рисков и смягчения их последствий.

4) *Владелец продукта*

- **Соответствие потребностям бизнеса**: Владелец продукта гарантирует, что закупаемые продукты или услуги соответствуют потребностям бизнеса и стратегическим целям. Это включает в себя проверку соответствия функций и возможностей продукта указанным требованиям.
- **Управление жизненным циклом продукта**: владелец отвечает за надзор за жизненным циклом продукта от закупки до развёртывания и далее, гарантируя, что продукт продолжает удовлетворять потребности организации по мере их развития

C. Этап после покупки

Этап включает в себя обеспечение того, чтобы приобретённые цифровые продукты и услуги по-прежнему соответствовали целям организации в области безопасности, оперативным и стратегическим целям. Этот этап требует постоянных оценок и управленческих практик для устранения любых возникающих рисков или изменений в среде организации или продукта.

1) *Высшее руководство*

- **Постоянное принятие и анализ рисков**: Высшее руководство должно установить процесс для постоянного или периодического принятия и анализа рисков продукта. Это включает в себя обеспечение того, чтобы управление рисками продукта осуществлялось в реестре рисков организации, а планы обеспечения безопасности системы и непрерывности бизнеса обновлялись и принимались.
- **Управление устаревшими технологиями**: Высшее руководство также должно учитывать риски, связанные с устаревшими технологиями, обеспечивая их документирование и надлежащее управление в рамках системы управления рисками организации.

2) *Системное администрирование*

- **Мониторинг обновлений системы безопасности**: Системные администраторы отвечают за настройку систем мониторинга и уведомлений об исправлениях, CVE и обновлениях продуктов, включая те, которые связаны со всей цепочкой поставок. Это гарантирует, что организация по-прежнему осведомлена о новых уязвимостях или обновлениях и может реагировать на них.
- **Интеграция с SIEM и SOAR**: Продукт должен быть интегрирован в систему организации SIEM (информация о безопасности и управление событиями), и, если применимо, должны быть предоставлены возможности SOAR (управление безопасностью, автоматизация и реагирование). Эта интеграция помогает обнаруживать инциденты безопасности и реагировать на них.
- **Процедуры управления данными**: Процедуры управления данными, включая удаление, редактирование и резервное копирование, должны быть установлены и соблюдаться для защиты целостности и конфиденциальности данных.
- **Включение плана реагирования на инциденты**: Новый продукт или услуга должны быть включены в план реагирования на инциденты организации, гарантируя наличие конкретных стратегий реагирования.

3) *Инфраструктура и безопасность*

- **Периодический пересмотр разрешений**: Организации следует периодически проверять разрешения и учётные записи с привилегиями, чтобы гарантировать, что средства контроля доступа остаются надлежащими и безопасными.
- **Проверка сертификатов безопасности производителя**: Сертификаты безопасности производителя следует периодически проверять на наличие обновлений, чтобы убедиться, что продукт продолжает соответствовать требуемым стандартам безопасности.
- **Управление устаревшими и новыми технологиями**: Организация план поддержки для управления как устаревшими, так и новыми технологиями, гарантирующий учёт рисков безопасности и эксплуатации.

4) *Владелец продукта*

- **Соблюдение производителем требований**: Владелец продукта должен убедиться, что производитель продолжает соблюдать требования по безопасности и эксплуатации, сделанные на этапе покупки.
- **Периодические проверки контрактов**: Контракты и соглашения об уровне обслуживания с производителем следует периодически пересматривать, чтобы обеспечить постоянное соответствие требованиям и учитывать любые изменения в потребностях организации или характеристиках продукта.
- **Оценка рисков изменений**: Любые изменения в продукте, включая обновления или изменения конфигурации, должны подвергаться оценке рисков, чтобы убедиться, что они не привносят новых уязвимостей или не ставят под угрозу безопасность.
- **Разработка планов обеспечения непрерывности и безопасности**: Владелец продукта должен обеспечить разработку и поддержание планов обеспечения непрерывности бизнеса и системной безопасности с учётом как нормативных, так и законодательных требований