DOI: 10.18372/2410-7840.22.14663
УДК 004.056

СРАВНЕНИЕ АРХИТЕКТУР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Михаил Коломыцев, Светлана Носок, Роман Тоцкий

Архитектура информационной безопасности помогает сопоставить текущее состояние обеспечения безопасности с желаемым и определить, как его достичь оптимальным образом. Архитектура информационной безопасности особенно важна в нестабильной экономической ситуации, когда денег на все, что «хочется», уже нет, и все проекты должны быть увязаны с выживанием бизнеса в условиях кризиса. Только четко выстроенная архитектура позволяет не сбиться с пути и достичь поставленных целей. Реализация архитектуры безопасности часто является сложным процессом на предприятиях. Традиционно архитектура безопасности состоит из некоторых превентивных, детективных и корректирующих элементов управления, которые применяются для защиты инфраструктуры предприятия и приложений. Некоторые предприятия работают лучше с архитектурой безопасности, добавляя директивные элементы управления, включая политики и процедуры. Многие специалисты по информационной безопасности с традиционным мышлением рассматривают архитектуру безопасности как не что иное, как наличие политик безопасности, элементов управления, инструментов и мониторинга. Сегодняшние факторы риска и угрозы не являются такими же и не такими простыми, какими они были раньше. Новые появляющиеся технологии и возможности, например, «IIнтернет вещей», сильно меняют то, как работают компании, каковы их цели и видение. Всем специалистам по безопасности важно понимать бизнес-цели и пытаться их поддерживать, внедряя надлежащие средства контроля, которые могут быть просто оправданы для заинтересованных сторон и связаны с бизнес-рисками. В статье будут проанализированы следующие архитектуры безопасности, которые могут помочь достичь таковой цели: SABSA. Sherwood Applied Business Security Architecture (SABSA); O-ESA. Открытая архитектура безопасности предприятия (O-ESA); OSA. Открытая архитектура безопасности (OSA).

Ключевые слова: *информационная безопасность; архитектура безопасности предприятия; атрибуты сравнения; предприятие; бизнес-цели, модель.*

АКТУАЛЬНОСТЬ И ПОСТАНОВКА ЗАДАЧИ

Цель данной статьи – описать и сравнить наиболее известные архитектуры информационной безопасности для использования предприятиями. В статье показано, что архитектуры информационной безопасности схожи между собой и предоставляют примерно равные возможности. Все они основываются на оценке рисков, хотя и на разных уровнях глубины. Было отмечено, что каждая архитектура в силу своей специфики имеет различные области применения.

Архитектура информационной безопасности – это термин, который применяется к широкому кругу деятельности, каждая из которых отличается по уровню детализации и организационному уровню, на котором она осуществляется. Поскольку такая деятельность порой различна, её рамки также могут сильно различаться как функционально, качественно. Чтобы организации могли принять обоснованное решение о правильной структуре архитектуры информационной безопасности, которая соответствует организационным потребностям, необходимы средства для сравнения.

Для этого исследования была поставлена задача:

– Определить понятие "архитектура информационной безопасности".

– Выбрать критерии сравнения архитектур.

– Провести анализ известных архитектур информационной безопасности для использования на предприятии.

Результат работы дает представление об архитектурах информационной безопасности, целях, которым они служат, и возможностями их использования. Это предоставляет организации достаточную информацию для принятия обоснованного решения о выборе подходящей архитектуры информационной безопасности.

1. АРХИТЕКТУРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Архитектура ИБ описывает процессы, роли людей, технологии и разные типы информации, а также учитывает сложность и изменчивость современного предприятия, адаптируясь к ним, но не ограничивая бизнес-возможности. Иными словами, она описывает желаемое состояние системы информационной безопасности организации и других компонентов и интерфейсов, связанных с ней. При этом архитектура ИБ должна отражать как текущие и, что очень важно, будущие потребности бизнеса, минимизируя соответствующие риски.

Для снижения рисков необходима архитектура информационной безопасности, учитывающая все особенности архитектуры предприятия. Разница между архитектурой предприятия и архитектурой информационной безопасности заключается в том, что архитектура предприятия имеет дело с одним уровнем: уровнем предприятия. Обычно выделяется 3 уровня архитектуры (независимо от того, относится она к информационной безопасности, ИТ или предприятию в целом) – стратегический или концептуальный, логический и системный или технологический (его еще часто называют уровнем реализации). Архитектуры информационной безопасности могут быть применимы на уровне предприятия, но также и на очень детальном уровне показывают объем мероприятия информационной безопасности для организации.

Информационная безопасность обычно описывается с использованием трех основных атрибутов [1]:

– Целостность. FIPS PUB 199 описывает целостность как: «Защита от неавторизованного изменения или уничтожения информации, и включает в себя обеспечение достоверности и невозможности отказа от авторства».

– Конфиденциальность. FIPS PUB 199 описывает конфиденциальность как: «Сохранение разрешенных ограничений на доступ к информации и ее раскрытия, включая средства защиты личной и конфиденциальной информации».

– Доступность. FIPS PUB 199 описывает доступность как: «Обеспечение своевременного и надежного доступа и использования информации».

Совокупность этих атрибутов называют КЦД-триадой. Часто включаются и другие характеристики ИБ, такие как достоверность (проверка подлинности), возможность учёта (прослеживаемость действий для уникальных лиц) и связанная с этим концепция невозможности отказа от авторства (невозможность отрицания того, что совершенные действия выполнены конкретным субъектом). Архитектура информационной безопасности направлена на то, чтобы эти базовые характеристики информационной безопасности адекватно учитывались в контексте предприятия на разных уровнях его архитектуры.

В общем, архитектура безопасности описывает и предоставляет руководство по защите информации. Это руководство может быть предоставлено на уровне бизнеса, на уровне информационных систем или на уровне технологий. В следующих разделах рассмотрим и классифицируем различные виды архитектуры информационной безопасности и уровень, на котором они действуют.

2. КРИТЕРИИ СРАВНЕНИЯ АРХИТЕКТУР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье будут проанализированы следующие архитектуры безопасности:

– SABSA. Sherwood Applied Business Security Architecture (SABSA) – это руководство и методология для создания архитектуры информационной безопасности, основанной на бизнес-требованиях и профиле рисков организации. Методология описывает использование метода анализа рисков и рекомендует, как использовать инфраструктуру для создания архитектуры безопасности. Руководство определяет принципы безопасности исходя из бизнес-требований к ИТ-компонентам. SABSA в достаточной мере пересекается с архитектурой Захмана [2]. Эта архитектура не будет отдельно анализироваться, а будет рассматриваться только как составная часть SABSA;

– O-ESA. Открытая архитектура безопасности предприятия (O-ESA) разработана The Open Group и предоставляет, согласно подзаголовку публикации: «основу и шаблон для обеспечения безопасности на основе политик» [3]. Она не предоставляет конкретной архитектуры информационной безопасности предприятия, а также не описывает полную методологию для реализаций. Вместо этого в ней рассматриваются области, на которые следует обратить внимание архитекторам информационной безопасности, и даются рекомендации по интеграции с корпоративной архитектурой;

– OSA. Открытая архитектура безопасности (OSA) предоставляет свободно доступное руководство, которое можно применять для создания архитектуры безопасности. Согласно декларации на сайте организации, задача OSA состоит в том, чтобы «раскрыть ноу-хау сообщества разработчиков архитектуры информационной безопасности и предоставить готовые шаблоны для использования» [4].

В этой статье используются следующие основные атрибуты для оценки архитектуры информационной безопасности:

– Конфиденциальность. Этот атрибут направлен на то, чтобы информация была доступна только тем, кто имеет на нее право просматривать.

Связанные методы включают шифрование, контроль доступа и авторизацию.

– Целостность. Этот атрибут призван гарантировать, что информация не будет изменена несанкционированным образом. Связанными методами являются хеширование, контроль доступа и цифровая подпись.

– Доступность. Этот атрибут направлен на то, чтобы информация была доступна уполномоченным лицам, когда она требуется. Связанные методы включают в себя ключевые слова: резервное копирование, резервирование и отработка отказа, подключение и аварийное восстановление.

– Подлинность. Этот атрибут предназначен для обеспечения подлинности (аутентичности) информации. Аутентичность информации – свойство, гарантирующее, что информационный ресурс идентичен заявленным. Таким образом, получатель должен иметь возможность проверить, что отправленное сообщение является действительным, а отправитель является тем, за кого он себя выдает. Следовательно, подлинность связана с целостностью. Связанные методы включают шифрование, цифровую подпись и цифровые сертификаты.

– Возможность учёта. Этот атрибут направлен на то, чтобы действия могли быть прослежены с точностью до конкретных лиц. Связанные методы включают ведение журнала, аудит и идентификацию.

– Невозможность отказа от авторства. Этот атрибут направлен на то, чтобы эти лица не могли отрицать действия, совершаемые ими. Концепция тесно связана с возможностью учёта. Связанные методы включают шифрование, цифровые подписи и инфраструктуры открытых ключей.

3. АНАЛИЗ АРХИТЕКТУР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В этом разделе описывается оценка трех архитектур с использованием ранее описанных атрибутов.

3.1. SABSA

Sherwood Applied Business Security Architecture была в первые введена в 2005 году. Она направлена на обеспечение четко определенного метода для достижения результатов в связанных с информационной безопасностью ИТ-проектах и инициативах, которые соответствуют целям предприятия.

Основная особенность модели SABSA – то, что все должно быть получено из анализа деловых требований с позиций безопасности. Модель представлена в виде уровней с верхним (контекстным) уровнем, являющимся деловой стадией определения требований. На контекстном уровне основное внимание уделяется бизнес-целям и методам управления рисками и анализу рисков, а не фактическим технологиям информационной безопасности. На этом уровне утверждается программа поддержки программы информационной архитектуры. На контекстном уровне основное внимание уделяется бизнес-целям и методам управления рисками и анализа рисков, а не фактическим технологиям информационной безопасности. В каждом более низком уровне определяется новый уровень абстракции и детализации, пройдя определение концептуальной архитектуры, логической сервисной архитектуры, физической архитектуры инфраструктуры и наконец в самом низком слое, выборе технологий и продуктов (составляющая архитектура). На этих уровнях определяются требования к механизмам информационной безопасности.

Методология позиционируется авторами как «библия архитектуры информационной безопасности» и предоставляет архитектору руководство по процессу построения архитектуры начиная с определения плана архитектуры информационной безопасности до структурирования и создания архитектуры, контроль процесса и результатов проведенных мероприятий. В методологии SABSA интенсивно используются сценарии использования, которые применяют архитектуру к реальным ситуациям, что дает практическое руководство по реализации.

Конфиденциальность

Конфиденциальность является одной из «служб безопасности», упомянутых SABSA для защиты информации на прикладном уровне и поддерживаемой несколькими из «шести А»: авторизация, аутентификация, контроль доступа (accesscontrol) и администрирование (связанное с контролем доступа). Конфиденциальность данных в базах данных также обеспечивается контролем доступа и разрешениями. «Стратегия аутентификации, авторизации и аудита», как указано в методологии, также связана с этим атрибутом, поскольку ограничение доступа к конфиденциальной информации только авторизованным и аутентифицированным лицам снизит вероятность несанкционированного доступа. SABSA гарантирует, что на последующих уровнях атрибут конфиденциальности и соответствующие механизмы также будут охвачены.

Целостность

Целостность также является одной из «служб безопасности», упомянутых SABSA для защиты информации на прикладном уровне. Концептуальная архитектура имеет дело с целостностью информации в базах данных и цифровой подписью через PKI, а также с механизмами контроля доступа, как упомянуто в предыдущем абзаце о конфиденциальности.

Доступность

Доступность кратко рассматривается в планировании резервного копирования и восстановления. Учитывая тот факт, что все темы, связанные с контролем доступа, помогают сохранить информацию доступной, гарантируя, что он не может быть удален неуполномоченными лицами, разделы по контролю доступа также применяются к доступности.

Подлинность

Как уже упоминалось, подлинность связана с целостностью. Она отдельно упоминается как одна из «служб безопасности» для защиты данных на уровне приложений. Поскольку подлинность может быть установлена с использованием методов PKI, применяется раздел о PKI. Аутентификация также может применяться, но только когда аутентификация связана с информацией, а не с пользователями или устройствами. На концептуальном уровне эта разница не всегда проясняется. Однако такие механизмы, как проверка подлинности, действительно указывают на то, что существует различие между аутентификацией пользователя и информации.

Возможность учёта

Возможность учёта не упоминается как одна из «служб безопасности» для защиты информации на прикладном уровне. Тем не менее, с возможностью учета тесно связана концепция невозможности отказа от авторства. Сама подотчетность рассматривается в стратегии «Аутентификация, авторизация и аудит», главным образом в теме «Аудит». Аудит гарантирует, что все действия, выполняемые отдельными лицами, регистрируются и хранятся в защищенном режиме. Подотчетность дополнительно поддерживается моделью управления доступом на основе ролей (RBAC), поскольку она обеспечивает централизованную систему управления пользователями. Централизованное управление пользователями и идентификацией помогает установить ответственность за действия.

Невозможность отказа от авторства

Невозможность отказа от авторства – это последняя из «служб безопасности», упомянутых SABSA для защиты информации на прикладном уровне. Так как невозможность отказа от авторства может быть достигнута с помощью криптографии и PKI, применяется весь раздел по теме PKI и раздел по подлинности.

3.2. O-ESA

Открытая архитектура безопасности предприятия (O-ESA) была впервые представлена как Архитектура корпоративной безопасности консорциума сетевых приложений (NAC ESA) в 2004 году. Члены консорциума предложили архитектуру информационной безопасности предприятия на основе политик, способную справляться со сложностями и быстрыми изменениями внутри предприятия. В 2011 году был пересмотрен NAC ESA, получивший название O-ESA, с подзаголовком: «Структура и шаблон для обеспечения безопасности на основе политик». В руководстве описывается подход к архитектуре информационной безопасности предприятия, который регулируется автоматизированным принятием решений на основе политики информационной безопасности. Эта концепция описана в руководстве как «обеспечение безопасности, основанная на политике».

O-ESA по сравнению с SABSA имеет другое назначение. В тех случаях, когда SABSA фокусируется на экономическом обосновании, а также на разработке, внедрении и эксплуатации различных методов обеспечения безопасности, O-ESA уделяет особое внимание внедрению платформы для операционной деятельности по обеспечению безопасности на основе политик. Тем не менее, эта структура учитывает некоторые методы обеспечения безопасности в примерах и службах безопасности.

Процесс построения архитектуры O-ESA включает в себя последовательную разработку концептуальной, логической и физической архитектур. Концептуальная архитектура – это концептуальная структура для управления принятием решений и политикой в широком спектре служб безопасности. В логической архитектуре подробно рассматриваются логические компоненты, необходимые для обеспечения служб безопасности. В физической архитектуре рассматриваются конкретные программные компоненты, обеспечивающие реализацию служб безопасности.

Конфиденциальность

Конфиденциальность рассматривается как одна из общих целей информационной безопасности и кратко упоминается в главе о принципах корпоративного управления. В конкретных примерах архитектуры в параграфах 4.4 (архитектура управления идентификационными данными) и 4.5 (архитектура защиты периметра) конфиденциальность рассматривается косвенным образом. Упомянутые компоненты архитектуры поддерживают конфиденциальность, обеспечивая контролируемый, аутентифицированный и авторизованный доступ к объектам. Эти компоненты предназначены для концептуальной, логической и физической архитектуры.

Целостность

Как и конфиденциальность, целостность рассматривается как одна из общих целей информационной безопасности и более подробно упоминается в разделе о принципах корпоративного управления. Конкретные примеры не касаются целостности напрямую, хотя можно утверждать, что механизмы контроля доступа защищают целостность, конфиденциальность и доступность информации. Таким образом, как архитектура управления идентификацией, так и архитектура защиты периметра способствуют сохранению целостности информации.

Доступность

Так же, как конфиденциальность и целостность, доступность рассматривается как одна из общих целей информационной безопасности. Доступность более подробно рассматривается в разделе об устойчивости. Доступность информации, конечно, зависит от надлежащего контроля доступа. Таким образом, ранее упомянутый раздел, в котором рассматривается управление доступом и связанные технологии (аутентификация, авторизация, идентификация), также способствуют обеспечению доступности.

Подлинность

Эта компонента безопасности не рассматривается в данной архитектуре информационной безопасности. Подтверждение подлинности не упоминается в качестве одной из основных целей информационной безопасности.

Возможность учёта

Эта компонента безопасности только косвенно рассматривается этой архитектурой информационной безопасности, хотя он упоминается как одна из целей управления информационной безопасностью. Есть раздел, посвященный управлению событиями и наблюдаемости, но он явно касается возможности учета. Скорее, этот раздел посвящен управлению инцидентами информационной безопасности. Можно утверждать, что управление идентификацией действительно способствует возможности учета, но поскольку другие базовые методы (такие как ведение журнала) не рассматриваются в контексте возможности учета, этот элемент не считается в достаточной степени раскрытым.

Невозможность отказа от авторства

Невозможность отказа от авторства не упоминается в этой архитектуре. Сервис PKI, рассмотренный в разделе архитектуры сервисов шифрования, можно использовать для невозможности отказа от авторства, но только в той части архитектуры, которая использует данный сервис. Это не считается достаточно широкой основой для полного обеспечения невозможности отказа от авторства.

3.3. OSA

Открытая архитектура безопасности (OSA) – это работа сообщества по архитектуре безопасности. Заявление на сайте OSA гласит (как упоминалось ранее): «OSA использует знания сообщества архитектуры безопасности и предоставляет готовые шаблоны для вашего приложения. OSA должна быть бесплатной платформой, разработанной и принадлежащей сообществу».

Сообщество архитектуры OSA определило некоторые строительные блоки, составляющие структуру архитектуры. Можно выделить следующие строительные блоки:

– Общая информация относительно области применения OSA. Эта информация включает в себя ландшафт архитектуры безопасности, основные принципы проектирования, на которых строилась OSA, и её таксономию.

– Элементы управления. OSA предоставляет набор элементов управления на основе стандарта NIST 800-53. Элементы управления хранятся в «контрольном каталоге» OSA.

– Шаблоны. OSA предоставляет несколько шаблонов безопасности, которые могут быть использованы архитектором информационной безопасности для разработки решений информационной безопасности. Шаблоны затрагивают широкий спектр тем и показывают, как их можно сопоставить с такими стандартами, как ISO27001 и

COBIT. Шаблоны хранятся в OSA «Каталог шаблонов».

– Угрозы. Одной из целей архитектуры информационной безопасности является в конечном итоге защита от угроз, с которыми сталкивается предприятие. Каталог угроз OSA содержит список соответствующих угроз, а также предоставляет метод оценки угроз.

Основные элементы информационной безопасности и сервисы в OSA упомянуты в библиотеке элементов управления. Однако библиотека элементов управления ограничивается присвоением имен элементам управления и ссылкам на стандарты безопасности.

Конфиденциальность

Конфиденциальность описывается OSA как одна из основных целей информационной безопасности. В библиотеке элементов управления, обеспечивающие конфиденциальность:

– Конфиденциальность передачи (SC-09).

– Средства управления, относящиеся к шифрованию:

1. Создание и управление криптографическим ключом (SC-12).

2. Использование криптографии (SC-13).

– Элементы управления, относящиеся к контролю доступа, в том числе:

1. Политики и процедуры контроля доступа (AC-01).

2. Обеспечение доступа (AC-03).

– Элементы управления, связанные с аутентификацией и авторизацией, включая:

1. Управление учетными записями (AC-02).

2. Политика идентификации и аутентификации и процедуры (IA-01).

3. Идентификация и авторизация пользователя (IA-02).

Целостность

Целостность также описывается OSA как одна из основных целей информационной безопасности. В библиотеке элементы управления, обеспечивающие целостность:

– Целостность передачи (SC-08).

– Политика и процедуры целостности системы и информации (SI-01).

– Целостность программного обеспечения и информации (SI-07).

– Элементы управления, относящиеся к управлению доступом (см. конфиденциальность).

– Элементы управления, относящиеся к шифрованию (см. конфиденциальность).

– Элементы управления, относящиеся к аутентификации и авторизации (см. конфиденциальность).

Доступность

Доступность – это последний элемент, описанный OSA как одна из основных целей информационной безопасности. В библиотеке элементами управления, обеспечивающие доступность информации:

– Все элементы управления, связанные с планированием на случай непредвиденных обстоятельств, в том числе:

1. Политики и процедуры планирования на случай непредвиденных обстоятельств (CP-01).

2. План на случай непредвиденных обстоятельств (CP-02).

3. Место альтернативного хранения (CP-06). Альтернативный узел обработки (CP-07).

4. Резервное копирование информационной системы (CP-09).

5. Восстановление и восстановление информационной системы (CP-10).

– Защита от отказа в обслуживании (SC-05).

– Все элементы управления, связанные с контролем доступа, см. Целостность и конфиденциальность.

Подлинность

Подлинность не упоминается как одна из основных целей информационной безопасности. Тем не менее, существуют элементы управления, которые специально предназначены для аутентификации:

– Точность, полнота, достоверность и аутентичность информации (SI-10).

– Аутентификация сеанса (SC-23).

Возможность учёта

Возможность учёта не упоминается как одна из основных целей информационной безопасности. Тем не менее, существуют средства управления, которые специально направлены на возможность учёта:

– Политика и процедуры аудита и подотчетности (AU-01).

– Все другие связанные с аудитом средства управления:

1. Аудиторские события (AU-02).

2. Содержание записей аудита (AU-03).

3. Аудиторские события (AU-03).

Невозможность отказа от авторства

Невозможность отказа от авторства не упоминается в качестве одной из основных целей информационной безопасности. Тем не менее, в разделе контроля и аудита есть особый элемент управления за невозможностью отказа от авторства, который так и называется: невозможность отказа от авторства (AU-10). Криптографические элементы управления могут также отнести к сервису невозможности отказа от авторства, в частности, к элементам управления, связанным с открытым ключом, таким как Установление и управление криптографическим ключом (SC-12) и Сертификаты инфраструктуры открытых ключей (SC-17).

4. РЕЗУЛЬТАТЫ ОЦЕНКИ

Оценка архитектуры информационной безопасности может быть выполнена с использованием модели на основе набора атрибутов, которые являются специфическими для архитектуры информационной безопасности.

Таблица 1

Сравнение всех архитектур информационной безопасности по основным атрибутам

№	Атрибут	SABSA	O-ESA	OSA
1	Конфиденциальность	+	+	+
2	Целостность	+	+	+
3	Доступность	+	+	+
4	Подлинность	+	-	+
5	Возможность учёта	+	-	+
6	Невозможность отказа от авторства	+	-	+

ЗАКЛЮЧЕНИЕ

В данной работе были решены следующие задачи:

– определено понятие архитектуры информационной безопасности, приемлемое с точки зрения дальнейшего анализа;

– определен перечень различных архитектур информационной безопасности на основе их известности и популярности;

– выбран критерий сравнения различных архитектур путем выбора атрибутов, важных с точки зрения информационной безопасности;

– проведен сравнительный анализ архитектур безопасности, позволяющий сделать обоснованный выбор в пользу одной из архитектур.

Можно утверждать, что наилучшей является архитектура SABSA, поскольку она включает в себя все рассматриваемые атрибуты, имеет ориентированность на бизнес-требования и позволяет обеспечить соответствие целям информационной безопасности целям бизнеса.

Архитектура OSA может быть использована как практическое руководство для внедрения, но применяемые в ней элементы управления информационной безопасности и их сопоставление стандартам не обновляется регулярно.

Архитектура O-ESA также может быть использована, но не включает полный объем используемых атрибутов и требует некоторого улучшения.

ЛИТЕРАТУРА

[1]. FIPS, "Standards for Security Categorization of Federal Information and Information Systems", FIPS PUB 199.

[2]. J. Sherwood, A. Clark, D. Lynas, "Enterprise Security Architecture, A business-driven approach".

[3]. Open Enterprise Security Architecture (O-ESA), "A Framework and Template for PolicyDriven Security", [Electronic resource]. Online access: https://publications.opengroup.org/g112.

[4]. OSA, [Electronic resource]. Online access: http://www.opensecurityarchitecture.org.

COMPARISON OF INFORMATION SECURITY ARCHITECTURES

The information security architecture helps to compare the current state of security with the desired one and determine how to achieve it in an optimal way. The architecture of information security is especially important in an unstable economic situation when there is no more money for everything you “want”, and all projects should be linked to the survival of the business in a crisis. Only a clearly built architecture allows you to stay on track and achieve your goals. Implementing security architecture is often a complex process in enterprises. Traditionally, a security archi-

tecture consists of some preventive, detective, and corrective controls that are used to protect enterprise infrastructure and applications. Some enterprises work better with security architectures by adding policy-based controls, including policies and procedures. Many traditional information security thinkers see information security architecture as nothing more than the presence of security policies, controls, tools, and monitoring. The world has changed; information security is not the beast as before. Today's risk factors and threats are not as simple and not as simple as they were before. New emerging technologies and capabilities, such as the Internet of Things, are changing dramatically how companies work and what their goals and objectives are. It is important for all security professionals to understand business goals and try to support them by introducing appropriate controls that can simply be justified to interested parties and involve business risks. That is why, the concept of information security architecture is used. This article will analyze the following information security architectures that may help achieve this goal: SABSA. Sherwood Applied Business Security Architecture (SABSA); O-ESA. Open Enterprise Security Architecture (O-ESA); OSA. Open Security Architecture (OSA).
Keywords: information security, architecture, comparison attributes, company, business goals, model.

ПОРІВНЯННЯ АРХІТЕКТУР ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Архітектура інформаційної безпеки допомагає зіставити поточний стан забезпечення безпеки з бажаним і визначити, як його досягти оптимальним чином. Архітектура інформаційної безпеки особливо важлива в нестабільній економічній ситуації, коли грошей на все, що «хочеться», вже немає, і всі проекти повинні бути пов'язані з виживанням бізнесу в умовах кризи. Тільки чітко вибудувана архітектура дозволяє не збитися зі шляху і досягти поставлених цілей. Реалізація архітектури інформаційної безпеки часто є складним процесом на підприємствах. Традиційно архітектура інформаційної безпеки складається з деяких превентивних, детективних і коригувальних елементів управління, які застосовуються для захисту інфраструктури підприємства і додатків. Деякі підприємства працюють краще з архітектурою інформаційної безпеки, додаючи директивні елементи управління, включаючи політики і процедури. Багато фахівців з інформаційної безпеки з традиційним мисленням розглядають архітектуру безпеки як ніщо інше, як наявність політик безпеки, елементів управління, технічних інструментів і моніторингу. Сьогоднішні фактори ризику і загрози не є такими ж і не такими простими, якими вони були раніше. Нові технології, що з'являються і можливості, наприклад, «Інтернет речей», сильно змінюють те, як працюють компанії, які їхні цілі і бачення. Всім фахівцям з безпеки важливо розуміти бізнес-цілі і намагатися їх підтримувати, впроваджуючи належні засоби контролю, які можуть бути просто аргументовані для зацікавлених сторін і пов'язані з бізнес-ризиками. Для цього використовують поняття архітектури інформаційної безпеки. У статті будуть проаналізовані наступні архітектури безпеки, які можуть допомогти досягти такої мети: SABSA. Sherwood Applied Business Security Architecture (SABSA); O-ESA. Відкрита архітектура безпеки підприємства (O-ESA); OSA. Відкрита архітектура безпеки (OSA).
Ключові слова: інформаційна безпека, архітектура, атрибути порівняння, підприємство, бізнес-цілі, модель.

Коломиец Михайло Володимирович, кандидат технічних наук, доцент Фізико-технічного інституту НТУУ «КПІ».
E-mail: box144.85@gmail.com.
Orcid ID: 0000-0001-8460-3041.
Коломыцев Михаил Владимирович, кандидат технических наук, доцент Физико-технического института НТУУ «КПИ».
Kolomytsev Myhailo, candidate of technical sciences, associate professor of Institute of Physics and Technologies of the NTUU "KPI".

Носок Світлана Олександрівна, кандидат технічних наук, доцент Фізико-технічного інституту НТУУ «КПІ».
E-mail: nos.sv.ol@gmail.com.
Orcid ID: 0000-0002-0016-9346.
Носок Светлана Александровна, кандидат технических наук, доцент Физико-технического института НТУУ «КПИ»
Nosok Svitlana, candidate of technical sciences, associate professor of Institute of Physics and Technologies of the NTUU "KPI".

Тоцький Роман Олександрович, студент Фізико-технічного інституту НТУУ «КПІ».
E-mail: r.totskyi@gmail.com.
Orcid ID: 0000-0001-9695-0681.
Тоцкий Роман Александрович, студент Физико-технического института НТУУ «КПИ».
Totskyi Roman, student of the Institute of Physics and Technologies of the NTUU "KPI".