###### Тема диплома: «ФУНКЦІОНАЛЬНі КОМПОНЕНТи для оцінки

###### БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Види робіт | Термін виконання | Формазвітності | Відмітка наукового керівника |
| 1 семестр | | | | |
| 1 | Основні засади управління конфігурацією та життєвим циклом системи захисту інформації |  |  |  |
| 2 | Аналіз стандартів в сфері ІБ та їх застосування: ISO/IEC 15408-1:2009; ISO/IEC 15408-2:2008; ISO/IEC 15408-3:2008; ISO/IEC 18045:2008 |  |  |  |
| 3 | Дослідити ключові поняття функціональних вимог інформаційної безпеки, які можуть бути предявлені до обєкту оцінки. |  |  |  |
| 4 | Дослідити структуру функціонального класу (сімейства, компоненту) інформаційної безпеки |  |  |  |
| 2 семестр | | | | |
| 5 | Підготовка статей по темі роботи |  |  |  |
| 6 | Доповідь по темі роботи на науково-технічних конференціях |  |  |  |
| 7 | Оформлення роботи і представлення на перевірку |  |  |  |
| 8 | Представлення роботи рецензенту |  |  |  |
| 9 | Захист роботи |  |  |  |

1. **Основні засади управління конфігурацією та життєвим циклом системи захисту інформації**

Определение информационной безопасности

Прежде чем разрабатывать стратегию информационной безопасности, необходимо принять базовое определение самого понятия, которое позволит применять определенный набор способов и методов защиты.

Практики отрасли предлагают понимать под информационной безопасностью стабильное состояние защищенности информации, ее носителей и инфраструктуры, которая обеспечивает целостность и устойчивость процессов, связанных с информацией, к намеренным или непреднамеренным воздействиям естественного и искусственного характера. Воздействия классифицируются в виде угроз ИБ, которые могут нанести ущерб субъектам информационных отношений.

Таким образом, под защитой информации будет пониматься комплекс правовых, административных, организационных и технических мер, направленных на предотвращение реальных или предполагаемых ИБ-угроз, а также на устранение последствий инцидентов. Непрерывность процесса защиты информации должна гарантировать борьбу с угрозами на всех этапах информационного цикла: в процессе сбора, хранения, обработки, использования и передачи информации.

Информационная безопасность в этом понимании становится одной из характеристик работоспособности системы. В каждый момент времени система должна обладать измеряемым уровнем защищенности, и обеспечение безопасности системы должно быть непрерывным процессом, которые осуществляется на всех временных отрезках в период жизни системы.

В теории информационной безопасности под субъектами ИБ понимают владельцев и пользователей информации, причем пользователей не только на постоянной основе (сотрудники), но и пользователей, которые обращаются к базам данных в единичных случаях, например, государственные органы, запрашивающие информацию. В ряде случаев, например, в банковских ИБ-стандартах к владельцам информации причисляют акционеров – юридических лиц, которым принадлежат определенные данные

Поддерживающая инфраструктура, с точки зрения основ ИБ, включает компьютеры, сети, телекоммуникационное оборудование, помещения, системы жизнеобеспечения, персонал. При анализе безопасности необходимо изучить все элементы систем, особое внимание уделив персоналу как носителю большинства внутренних угроз.

Основные постулаты, которые не утратили своей актуальности и по сей день.

Первый постулат гласит: абсолютно надежную, непреодолимую защиту создать нельзя. Система защиты информации (СЗИ) может быть в лучшем случае адекватна потенциальным угрозам. Поэтому при планировании защиты необходимо представлять, кого и какая именно информация может интересовать, какова ее ценность для вас и на какие финансовые жертвы ради нее способен пойти злоумышленник.

Из первого постулата вытекает второй: СЗИ должна быть комплексной, т. е. использующей не только технические средства защиты, но также административные и правовые.

Третий постулат состоит в том, что СЗИ должна быть гибкой и адаптируемой к изменяющимся условиям. Главную роль в этом играют административные (или организационные) мероприятия, такие, например, как регулярная смена паролей и ключей, строгий порядок их хранения, анализ журналов регистрации событий в системе, правильное распределение полномочий пользователей и многое другое. Человек, отвечающий за все эти действия, должен быть не только преданным сотрудником, но и высококвалифицированным специалистом как в области технических средств защиты, так и в области вычислительных средств вообще.

Рассмотрим, какие же направления защиты и соответствующие им технические средства вызывают сегодня наибольшее внимание со стороны разработчиков и потребителей.

* Защита от несанкционированного доступа (НСД) ресурсов автономно работающих и сетевых ПК. Эта функция реализуется программными, программно-аппаратными и аппаратными средствами, которые будут рассмотрены ниже на конкретных примерах.
* Защита серверов и отдельных пользователей сети Internet от злонамеренных хакеров, проникающих извне. Для этого используются специальные межсетевые экраны (брандмауэры), которые в последнее время приобретают все большее распространение.
* Защита секретной, конфиденциальной и личной информации от чтения посторонними лицами и целенаправленного ее искажения осуществляется чаще всего с помощью криптографических средств, традиционно выделяемых в отдельный класс. Сюда же можно отнести и подтверждение подлинности сообщений с помощью электронной цифровой подписи (ЭЦП). Применение криптосистем с открытыми ключами и ЭЦП имеет большие перспективы в банковском деле и в сфере электронной торговли. Достаточно широкое распространение в последние годы приобрела защита ПО от нелегального копирования с помощью электронных ключей. В данном обзоре она также рассмотрена на конкретных примерах.
* Защита от утечки информации по побочным каналам (по цепям питания, каналу электромагнитного излучения от компьютера или монитора). Здесь применяются такие испытанные средства, как экранирование помещения и использование генератора шума, а также специальный подбор мониторов и комплектующих компьютера, обладающих наименьшей зоной излучения в том частотном диапазоне, который наиболее удобен для дистанционного улавливания и расшифровки сигнала злоумышленниками.
* Защита от шпионских устройств, устанавливаемых непосредственно в комплектующие компьютера, так же как и измерения зоны излучения, выполняется спецорганизациями, обладающими необходимыми лицензиями компетентных органов.

### **Вимоги до архітектури інформаційної системи для забезпечення безпеки її функціонування**

Ідеологія відкритих систем (див. гол. 19) суттєво вплинула на методологічних аспектах і напрямку розвитку складних ІС. Вона базується на суворому дотриманні сукупності профілів, протоколів і стандартів де-факто і де-юре. Програмні і апаратні компоненти цієї ідеології повинні відповідати найважливішим вимогам переносимості та можливості узгодженої спільної роботи з іншими віддаленими компонентами. Це дозволяє забезпечити сумісність різних компонент інформаційних систем, а також засобів передачі даних. Завдання зводиться до максимально можливого повторного використання розроблених і апробованих програмних та інформаційних компонент при зміні обчислювальних апаратних платформ, ОС і процесів взаємодії.

При створенні складних, розподілених інформаційних систем, їх проектуванні архітектури, інфраструктури, виборі компонентів і зв'язків між ними слід враховувати крім загальних (відкритість, масштабованість, переносимість, мобільність, захист інвестицій тощо) ряд специфічних концептуальних вимог, спрямованих на забезпечення безпеки функціонування:

o архітектура системи повинна бути достатньо гнучкою, тобто повинна допускати відносно просте, без докорінних структурних змін, розвиток інфраструктури і зміна конфігурації використовуваних засобів, нарощування функцій і ресурсів ІС відповідно з розширенням сфер і завдань її застосування;

o повинні бути забезпечені безпека функціонування системи при різних видах загроз і надійний захист даних від помилок проектування, руйнування або втрати інформації, а також авторизація користувачів, керування робочої завантаженням, резервуванням даних і обчислювальних ресурсів, максимально швидким відновленням функціонування ІС;

o слід забезпечити комфортний, максимально спрощений доступ користувачів до сервісів і результатами функціонування ІС на основі сучасних графічних засобів, мнемосхем та наочних користувальницьких інтерфейсів;

o систему повинна супроводжувати актуалізована, комплектна документація, що забезпечує кваліфіковану експлуатацію і можливість розвитку ІС.

Підкреслимо, що системи безпеки, якими б потужними вони не були, самі по собі не можуть гарантувати надійність програмно-технічного рівня захисту. Тільки перевірена архітектура здатна зробити ефективним об'єднання сервісів, забезпечити керованість інформаційної системи, її здатність розвиватися і протистояти новим загрозам при збереженні таких властивостей, як висока продуктивність, простота і зручність використання.

З практичної точки зору забезпечення безпеки найбільш важливими є наступні принципи побудови архітектури ІС:

o проектування ІС на принципах відкритих систем, дотримання визнаним стандартам, використання апробованих рішень, ієрархічна організація ІС з невеликим числом сутностей на кожному рівні - все це сприяє прозорості і хорошої керованості ІС;

o безперервність захисту в просторі і часі, неможливість подолати захисні засоби, виключення спонтанного або викликаного переходу в небезпечний стан - при будь-яких обставин, у тому числі позаштатних, захисне засіб або цілком виконує свої функції, або цілком блокує доступ до системи або її частина;

o посилення самої слабкої ланки, мінімізація привілеїв доступу, поділ функцій обслуговуючих сервісів і обов'язків персоналу. Передбачається такий розподіл ролей і відповідальності, щоб одна людина не може порушити критично важливий для організації процес або створити пролом у захисті з незнання або замовлення зловмисників. Стосовно до програмно-технічному рівню принцип мінімізації привілеїв наказує виділяти користувачам і адміністраторам тільки ті права доступу, що необхідні їм для виконання службових обов'язків. Це дозволяє зменшити шкоду від випадкових або навмисних некоректних дій користувачів та адміністраторів;

o ешелонування оборони, розмаїтість захисних засобів, простота і керованість інформаційної системи і системою її безпеки. Принцип ешелонування оборони наказує не покладатися на один захисний рубіж, яким би надійним він ні здавався. За засобами фізичного захисту повинні випливати программнотехнические засоби, за ідентифікацією і аутентифікацією - управління доступом, протоколювання й аудит. Ешелонована оборона здатна не тільки не пропустити зловмисника, але і в деяких випадках ідентифікувати його завдяки протоколювання і аудиту. Принцип розмаїтості захисних засобів передбачає створення різних за характером оборонних рубежів, щоб від потенційного зловмисника було потрібно оволодіння різноманітними і, по можливості, несумісними між собою навичками.

Дуже важливий загальний принцип простоти і керованості ІС в цілому і захисних засобів в особливості. Тільки в простій і керованій системі можна перевірити погодженість конфігурації різних компонентів і здійснювати централізоване адміністрування. У цьому зв'язку важливо відзначити інтегруючу роль web-сервісу, що ховає розмаїтість об'єктів, що обслуговуються, і надає єдиний, наочний інтерфейс. Відповідно, якщо об'єкти деякого виду (наприклад, таблиці бази даних) доступні через Інтернет, необхідно заблокувати прямий доступ до них, оскільки в противному випадку система буде вразливою, складною і погано керованою.

Продумана і впорядкована структура програмних засобів і баз даних, топології внутрішніх і зовнішніх мереж безпосередньо відбивається на що досягає якості і безпеки ІС, а також на трудомісткість їх розробки. При строгому дотриманні правил структурної побудови значно полегшується досягнення високих показників якості і безпеки, так як скорочується число можливих помилок в реалізують програмах, відмов і збоїв устаткування, спрощується їх діагностика і локалізація. У добре структурованої системи з чітко виділеними компонентами (клієнт, сервер додатків, ресурсний сервер) контрольні точки виділяються досить чітко, що вирішує задачу докази достатності застосовуваних засобів захисту і забезпечення неможливості обходу цих коштів потенційним порушником.

Високі вимоги, пропоновані до формування архітектури та інфраструктури на стадії проектування ІС, визначаються тим, що саме на цій стадії можна значною мірою мінімізувати число вразливостей, пов'язаних з непредумышленными дестабілізуючими факторами, які впливають на безпеку програмних засобів, баз даних і систем комунікації.

Аналіз безпеки ІС при відсутності злочинних факторів базується на моделі взаємодії основних компонентів ІС (рис. 1).

В якості об'єктів уразливості розглядаються:

o динамічний обчислювальний процес обробки даних, автоматизованої підготовки рішень і вироблення керуючих впливів;

o об'єктний код програм, виконуваних обчислювальними засобами в процесі функціонування ІС;

o дані та інформація, накопичена в базах даних;

o інформація, яка видається споживачам і на виконавчі механізми.



***Рис. 1*Модель аналізу безпеки ІС при відсутності злочинних загроз**

### Етапи побудови системи безпеки ІС

Концепція інформаційної безпеки визначає етапи побудови системи інформаційної безпеки у відповідності зі стандартизованих життєвим циклом ІС: аудит безпеки (обстеження) існуючої системи захисту ІВ, аналіз ризиків, формування вимог і вироблення першочергових заходів захисту, проектування, впровадження, атестація, супровід системи. Розглянемо коротко зміст окремих етапів.

**Аудит безпеки.**Аудит безпеки може включати в себе, принаймні, чотири різні групи робіт.

До ***першої групи*** належать так звані тестові зломи ІС. Ці тести застосовуються, як правило, на початкових стадіях обстеження захищеності ІС. Причина малої ефективності тестових зломів ховається в самій постановці завдання. Дійсно, основним завданням зломщика є виявлення декількох вразливостей і їх використання для доступу в систему. Якщо тест виявився успішним, то, запобігши потенційний розвиток можливих сценаріїв злому, роботу треба починати спочатку і шукати такі. Неуспіх злому може означати в рівній мірі як захищеність системи, так і недостатність тестів.

***Друга група -*** експрес-обстеження. В рамках цього, звичайно нетривалої роботи оцінюється загальний стан механізмів безпеки в обстежуваній ІС на основі стандартизованих перевірок. Експрес-обстеження зазвичай проводиться у разі, коли необхідно визначити пріоритетні напрями, що дозволяють забезпечити мінімальний рівень захисту інформаційних ресурсів. Основу для нього складають списки контрольних питань, що заповнюються в результаті інтерв'ювання, так і тестової роботи автоматизованих сканерів захищеності.

***Третя група робіт з аудиту*** - атестація систем на відповідність вимогам захищеності інформаційних ресурсів. При цьому відбувається формальна перевірка набору вимог як організаційного, так і технічного аспектів, розглядаються повнота і достатність реалізації механізмів безпеки. Типова методика аналізу корпоративної інформаційної захищеності складається з сукупності наступних методів:

o вивчення вихідних даних за структурою, архітектури, інфраструктури та конфігурації ІС на момент обстеження;

o попередня оцінка ризиків, пов'язаних із здійсненням загроз відносно технічних та інформаційних ресурсів;

o аналіз механізмів безпеки організаційного рівня, політики безпеки організації і організаційно-распоряди

тельний документації щодо забезпечення режиму ІБ і оцінка їх відповідності вимогам існуючих стандартів і нормативних документів, а також їх адекватності існуючим ризикам;

o аналіз конфігураційних файлів маршрутизаторів і Ргоху-серверів, поштових і DNS-сервери (Domain Name System), шлюзів віртуальних приватних мереж (VPN), інших критичних елементів мережевої інфраструктури;

o сканування зовнішніх мережевих адрес локальної мережі;

o сканування ресурсів локальної мережі зсередини;

o аналіз конфігурації серверів і робочих станцій з допомогою спеціалізованих програмних агентів.

Перераховані технічні методи передбачають застосування як активного, так і пасивного тестування системи захисту. Активне тестування полягає в моделюванні дій потенційного зловмисника; а ***пасивне -*** передбачає аналіз конфігурації ОС і додатків за шаблонами з використанням списків перевірки. Тестування може проводитися вручну або з використанням спеціалізованих програмних засобів.

При аналізі конфігурації засобів захисту для зовнішнього периметра локальної мережі і управління міжмережними взаємодіями особлива увага звертається на наступні аспекти:

o налаштування правил розмежування доступу (фільтрація мережевих пакетів);

o схеми та налаштування параметрів аутентифікації;

o настройка параметрів системи реєстрації подій;

o використання механізмів, що забезпечують приховування топології мережі, яка захищається (наприклад, трансляція мережевих адрес);

o налагодження механізмів оповіщення про атаки і реагування;

o наявність і працездатність засобів контролю цілісності;

o версії використовуваного ЗА і встановлені оновлення.

Аналіз конфігурації передбачає перевірку правильності установки сотень різних параметрів. Для автоматизації цього процесу можуть використовуватися спеціалізовані програмні засоби аналізу захищеності, вибір яких в даний час досить широкий.

Один із сучасних і швидко розвиваються методів автоматизації процесів аналізу і контролю захищеності розподілених комп'ютерних систем - використання технології інтелектуальних програмних агентів. На кожну з контрольованих систем встановлюється програмний агент, який виконує відповідні налаштування, перевіряє їх правильність, контролює цілісність файлів, своєчасність установки оновлень, а також вирішує інші завдання з контролю захищеності ІС. Управління агентами здійснює по мережі програма-менеджер. Такі менеджерм, які є центральними компонентами таких систем, посилають керуючі команди всім агентам контрольованого ними домену і зберігають всі отримані від агентів дані в центральній БД. Адміністратор керує менеджерами за допомогою графічної консолі, що дозволяє вибирати, змінювати та створювати політики безпеки, аналізувати зміни стану системи, здійснювати ранжування вразливостей і т. п. Все взаємодії між агентами, менеджерами і керуючої консолі здійснюються по захищеному клієнт-серверному протоколу. Такий підхід, наприклад, використаний при побудові комплексної системи управління безпекою організації ESM (виробник - компанія "Symantec Enterprise Security Manager").

***Четверта група -*** перед проектне обстеження - самий трудомісткий варіант аудиту. Такий аудит передбачає аналіз організаційної структури підприємства в додатку до ІР, правила доступу співробітників до тих або іншим додаткам. Потім виконується аналіз самих додатків. Після цього повинні враховуватися конкретні служби доступу з одного рівня на інший, а також служби, необхідні для інформаційного обміну. Потім картина доповнюється вбудованими механізмами безпеки, що в поєднанні з оцінками втрат у разі порушення ІБ дає підстави для ранжирування ризиків, які існують в ІС, і вироблення адекватних контрзаходів. Успішне проведення передпроектного обстеження, подальшого аналізу ризиків і формування вимог визначають, наскільки прийняті заходи будуть адекватні погрозам, ефективні і економічно виправдані.

**Проектування системи.**В даний час склалися два підходи до побудови системи ІБ: продуктовий і проектний. В рамках ***продуктового*** підходу вибирається набір засобів фізичної, технічної і програмної захисту (готове рішення), аналізуються функції, а на основі аналізу функцій визначається політика доступу в робочі та технологічні приміщення, до інформаційних ресурсів. Можна надходити навпаки: спочатку опрацьовується політика доступу, на основі якої визначаються функції, необхідні для її реалізації, і здійснюється вибір засобів і продуктів, що забезпечують виконання цих функцій. Вибір методів залежить від конкретних умов діяльності організації, її місцезнаходження, розташування приміщень, складу підсистем ІС, сукупності розв'язуваних завдань, вимог до системи захисту і т. д. Продуктовий підхід більш дешевий з точки зору витрат на проектування. Крім того, в деяких випадках він є єдино можливим в умовах дефіциту рішень або жорстких вимог нормативних документів на державному рівні (наприклад, для криптографічного захисту інформації в мережах спеціального призначення та урядових телефонних мережах застосовується тільки такий підхід). ***Проектний*** підхід свідомо більш повний, і рішення, побудовані на його основі, зручніша і простіше аттестуемы. Він краще і при створенні великих гетерогенних розподілених систем, оскільки на відміну від продуктового підходу не пов'язаний спочатку з тією чи іншою платформою. Крім того, він забезпечує більш "довгоживучі" рішення, оскільки допускає проведення заміни продуктів і рішень без зміни політики доступу. Це, в свою чергу, забезпечує хороший показник повернення інвестицій (ROI) при розвитку ІС і системи ІБ.

**Об'єкти або програми?**При проектуванні архітектури системи інформаційної безпеки застосовуються об'єктний, прикладної або змішаний підходи.

***Об'єктний*** підхід будує захист інформації на підставі фізичної структури того чи іншого об'єкта (будівлі, підрозділу, підприємства). Застосування об'єктного підходу припускає використання набору універсальних рішень для забезпечення механізмів безпеки, підтримують однорідний набір організаційних заходів. Класичним прикладом такого підходу є побудова захищених інфраструктур зовнішнього інформаційного обміну, локальної мережі, системи телекомунікацій і т. д. До його недоліків відносяться очевидна неповнота універсальних механізмів, особливо для організацій з великим набором складно пов'язаних між собою програм.

***Прикладний*** підхід "прив'язує" механізми безпеки до конкретного додатка. Приклад такого підходу - захист підсистеми або окремих зон автоматизації (бухгалтерія, склад, кадри, проектне бюро, аналітичний відділ, відділи маркетингу і продажів тощо). При більшій повноті захисних заходів такого підходу у нього є і недоліки, а саме: необхідно пов'язувати різні за функціональним можливостям засоби безпеки для мінімізації витрат на адміністрування та експлуатацію, а також задіяти вже існуючі засоби захисту інформації для збереження інвестицій.

Можлива комбінація двох описаних підходів. У ***змішаному*** підході ІС представляється як сукупність об'єктів, для кожного з яких застосовано об'єктний підхід, а для сукупності взаємозалежних об'єктів - прикладної. Така методика виявляється більш трудомісткою на стадії проектування, однак часто дає хорошу економію коштів при впровадженні, експлуатації та супроводу системи захисту інформації.

**Служби і механізми безпеки.**Стратегію захисту можна реалізувати двома методами: ресурсним і сервісним. Перший метод розглядає ІС як набір ресурсів, які "прив'язуються" до конкретних компонентів системи ІБ. Цей метод хороший для невеликих ІС з обмеженим набором завдань. При розширенні кола завдань і розростанні ІС доводиться багато в чому дублювати елементи захисту для однотипних ресурсів, що часто призводить до невиправданих витрат. Сервісний підхід трактує ІС як набір служб, програмних і телекомунікаційних сервісів для надання послуг користувачам. У цьому випадку один і той же елемент захисту можна використовувати для різних сервісів, побудованих на одному і тому ж або технічному пристрої. Сьогодні сервісний підхід видається кращим, оскільки він припускає строгий функціональний аналіз існуючих численних служб, що забезпечують функціонування ІС, і дозволяє виключити широкий клас загроз за допомогою відмови від "зайвих" служб і оптимізації роботи залишилися, роблячи структуру системи ІБ логічно обґрунтованою. Саме сервісний підхід лежить в основі сучасних стандартів щодо безпеки, зокрема ISO 15408.

**Впровадження та атестація.**Етап впровадження включає в себе комплекс послідовно проведених заходів, у тому числі установку і конфігурування засобів захисту, навчання персоналу роботі із засобами захисту, проведення попередніх випробувань і здачу в дослідну експлуатацію. Дослідна експлуатація дозволяє виявити і усунути можливі недоліки функціонування підсистеми інформаційної безпеки, перш ніж запустити систему в "бойовій" режим. Якщо в процесі дослідної експлуатації виявлені факти некоректної роботи компонентів, проводять коригування налаштувань засобів захисту, режимів їх функціонування і т. п. За результатами дослідної експлуатації вносять коригування (за необхідності) і уточнюють налаштування засобів захисту. Далі слід проведення приймально-здавальних випробувань, введення в штатну експлуатацію і надання технічної підтримки і супроводу.

Підтвердження функціональної повноти системи безпеки і забезпечення необхідного рівня захищеності ІС забезпечується проведенням атестації системи ІБ відповідним акредитованим центром Федеральної служби з технічного та експортного контролю або зарубіжної незалежною лабораторією. Атестація передбачає комплексну перевірку захищеного об'єкта в реальних умовах експлуатації для оцінки відповідності застосовуваного комплексу заходів і засобів захисту необхідному рівню безпеки. Атестація проводиться згідно зі схемою, що складається на підготовчому етапі виходячи з наступного переліку робіт:

o аналіз вихідних даних, попереднє ознайомлення з атестуються об'єктом та інформатизації;

o експертне обстеження об'єкта інформатизації та аналіз документації з питань захисту інформації на предмет відповідності вимогам;

o випробування окремих засобів і систем захисту інформації на аттестуемом об'єкті за допомогою спеціальної контрольної апаратури і тестових засобів;

o випробування окремих засобів і систем захисту інформації у випробувальних центрах (лабораторіях);

o комплексні атестаційні випробування об'єкта інформатизації в реальних умовах експлуатації;

o аналіз результатів експертного обстеження та атестаційних випробувань і затвердження висновку за результатами атестації об'єкта інформатизації.

За результатами випробувань готується звітна документація, проводиться оцінка результатів випробувань і видається атестат відповідності встановленого зразка. Його наявність дає право обробки інформації зі ступенем конфіденційності та на період часу, встановленими в атестаті.

**Технічна підтримка та супровід.**Для підтримки працездатності підсистеми інформаційної безпеки та безперебійного виконання їй своїх функцій необхідно передбачити комплекс заходів з технічної підтримки та супроводу програмного і апаратного забезпечення підсистеми інформаційної безпеки, включаючи поточне адміністрування, роботи, що проводяться в екстрених випадках, а також періодично проводяться профілактичні роботи. Цей комплекс заходів включає в себе:

o адміністрування штатних засобів захисту та їх технічне обслуговування;

o контроль стану системи, профілактичне обстеження конфігурації, виявлення потенційних проблем;

o моніторинг та встановлення випущених оновлень і програмних корекцій засобів захисту, а також використовуваних ОС, СУБД і додатків;

o регулярний пошук і аналіз вразливостей в захищається системі з використанням спеціальних засобів сканування;

o діагностику несправностей та проведення відновних робіт при виникненні аварійних і позаштатних ситуацій;

o періодичне тестування системи інформаційної безпеки та оцінка ефективності захисту.

Технічна підтримка та супровід системи інформаційної безпеки вимагає наявності у обслуговуючого персоналу певних знань і навичок і може здійснюватися як штатними працівниками організації - власника ІВ, відповідальними за інформаційну безпеку, так і співробітниками спеціалізованих організацій.

1. **Аналіз стандарту ISO/IEC 15408**

Стандарт ISO 15408 — один из наиболее распространенных стандартов в области безопасности. В его создании приняли участие организации из США, Канады, Англии, Франции, Германии, Голландии. В стандарте, получившем название «Общие критерии оценки безопасности информационных технологий» (The Common Criteria for Information Technology Security Evaluation), подробно рассмотрены общие подходы, методы и функции обеспечения защиты информации в организациях.

Функции системы информационной безопасности обеспечивают выполнение требований конфиденциальности, целостности, достоверности и доступности информации. Все функции представлены в виде четырехуровневой иерархической структуры: класс — семейство — компонент — элемент. По аналогии представлены требования качества. Подобная градация позволяет описать любую систему информационной безопасности и сопоставить созданную модель с текущим положением дел.

В стандарте выделены 11 классов функций: аудит, идентификация и аутентификация, криптографическая защита, конфиденциальность, передача данных, защита пользовательских данных, управление безопасностью, защита функций безопасности системы, использование ресурсов, доступ к системе, надежность средств.

Оценка информационной безопасности базируется на моделях системы безопасности, состоящих из перечисленных в стандарте функций.

В ISO 15408 содержится ряд предопределенных моделей (так называемых профилей), описывающих стандартные модули системы безопасности. С их помощью можно не создавать модели распространенных средств защиты самостоятельно, изобретая велосипед, а пользоваться уже готовыми наборами описаний, целей, функций и требований к этим средствам. Простым примером профилей может служить модель межсетевого экрана или СУБД.

В мире уже создано и сертифицировано большое количество профилей. Каждый из них имеет отличительные черты, в том числе: область применения (например, профили «Контроль доступа» или «Программный межсетевой экран»); уровень надежности; статус сертификации (скажем, «проект», «в стадии разработки» или «сертифицирован»).

Сертифицированный профиль представляет собой полное описание определенной части (или функции) системы безопасности. В нем содержится анализ внутренней и внешней среды объекта, требования к его функциональности и надежности, логическое обоснование его использования, возможности и ограничения развития объекта.

Стандарт ISO 15408 выгодно отличает открытость. Описывающий ту или иную область системы безопасности профиль можно создать самостоятельно с помощью разработанной в ISO 15408 структуры документа. В стандарте определена также последовательность действий для самостоятельного создания профилей.

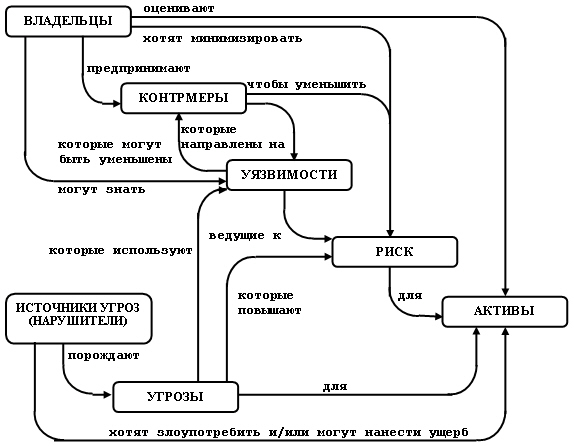


Рис Понятия безопасности и их взаимосвязь в соответствии с ИСО/МЭК 15408-1-2008

На рис.  представлена определяемая стандартом взаимосвязь высокоуровневых понятий в области ИБ. *Безопасность* связана с защитой активов ИС от угроз. За сохранность рассматриваемых активов отвечают их владельцы, для которых эти *активы* имеют ценность. Существующие или предполагаемые нарушители также могут придавать *значение* этим активам и стремиться использовать их вопреки интересам их владельца. Владельцы будут воспринимать подобные угрозы как *потенциал* воздействия на *активы*, приводящего к понижению их ценности для владельца.

Владельцы активов будут анализировать возможные угрозы, чтобы решить, какие из них действительно присущи их среде. В результате анализа определяются риски. *Анализ* может помочь при выборе контрмер для противостояния угрозам и *уменьшения рисков* до приемлемого уровня.

Контрмеры предпринимают для уменьшения уязвимостей и выполнения политики безопасности владельцев активов (прямо или косвенно распределяя между этими составляющими). Но и после введения этих контрмер могут сохраняться остаточные уязвимости. Такие уязвимости могут использоваться нарушителями, представляя уровень *остаточного риска* для активов. Владельцы будут стремиться минимизировать этот риск, задавая дополнительные ограничения.

Стандарт разработан таким образом, чтобы удовлетворить потребности трех групп специалистов: разработчиков, экспертов *по* сертификации и пользователей объекта оценки. Под объектом оценки (ОО) понимается "подлежащие *оценке продукт* информационных технологий (ИТ) или система с руководствами администратора и пользователя". К таким объектам относятся, например, операционные системы, прикладные программы, ИС и т.д.

"*Общие критерии*" предусматривают наличие двух типов требований безопасности - функциональных и доверия. 

*Функциональные требования* относятся к  *сервисам безопасности*, таким как *идентификация*, *аутентификация*, *управление доступом*, *аудит* и т.д. 

*Требования доверия* к безопасности относятся к технологии разработки, тестированию, *анализу уязвимостей*, поставке, сопровождению, эксплуатационной документации и т.д.

Описание обоих типов требований выполнено в едином стиле: они организованы в иерархию "*класс* - семейство - *компонент* - элемент". Термин "*класс*" используется для наиболее общей группировки требований безопасности, а элемент - самый нижний, неделимый уровень требований безопасности.

В стандарте выделены 11 классов функциональных требований:

* *аудит безопасности*;
* связь (передача данных);
* *криптографическая поддержка* (криптографическая защита);
* *защита данных пользователя*;
* *идентификация и аутентификация*;
* управление безопасностью;
* приватность (конфиденциальность);
* защита функций безопасности объекта;
* использование ресурсов;
* доступ к объекту оценки;
* *доверенный маршрут*/канал.

Основные структуры "Общих критериев" - это *профиль защиты* и задание *по* безопасности. *Профиль защиты* определяется как "независимая от реализации совокупность требований безопасности для некоторой категории ОО, отвечающая специфическим запросам потребителя". Профиль состоит из компонентов или пакетов функциональных требований и одного из уровней гарантированности. Структура профиля защиты представлена на [рис. 2.2](https://www.intuit.ru/studies/courses/531/387/lecture/8992?page=1#image.2.2).

Профиль определяет "модель" системы безопасности или отдельного ее модуля. Количество профилей потенциально не ограничено, они разрабатываются для разных областей применения (например, профиль "Специализированные средства защиты от несанкционированного доступа к конфиденциальной информации").

*Профиль защиты* служит основой для создания задания *по* безопасности, которое можно рассматривать как *технический проект* для разработки ОО. Задание *по* безопасности может включать требования одного или нескольких профилей защиты. Оно описывает также уровень функциональных возможностей средств и механизмов защиты, реализованных в ОО, и приводит обоснование степени их адекватности. *По* результатам проводимых оценок, создаются каталоги сертифицированных профилей защиты и продуктов (операционных систем, средств защиты информации и т.д.), которые затем используются при оценке других объектов.

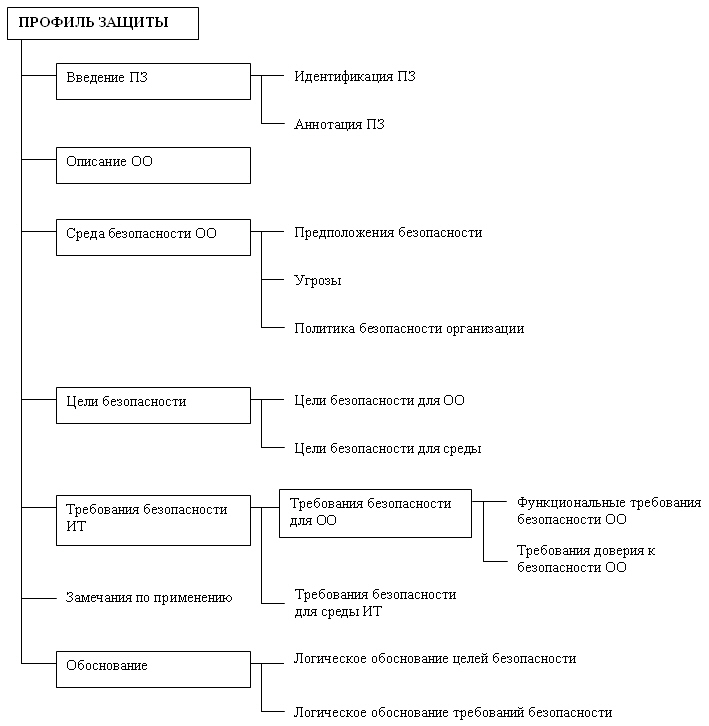


Рис Структура профиля защиты