Базовый уровень информационной безопасности

И.Л.Дмитриев
Член Оргкомитета Инфофорума

Структура доклада

- Понятие базового уровня безопасности
- Функциональные требования к подсистеме информационной безопасности (ПИБ)
- Технические требования к компонентам ПИБ
- Варианты реализации технических решений
- Требования к нормативному обеспечению ПИБ
- Требования к организационному обеспечению ПИБ
- Первоочередные мероприятия

Требования к базовому уровню безопасности

- В соответствии с международными стандартами (ISO 17799, ISO TR 13569 и др.) базовый уровень подразумевает следующий минимальный набор компонент подсистемы информационной безопасности:
  - защиты от несанкционированного доступа (НСД), управления доступом и регистрацией, в том числе при использовании средств телекоммуникаций и сети Интернет;
  - антивирусной защиты;
  - резервного копирования и восстановления информации;
  - криптографической защиты информации.
- Требования к базовому уровню безопасности включают:
  - функциональные требования (общие требования к подсистемам и технические требования к компонентам системы защиты информации),
  - требования по нормативному обеспечению,
  - требования по организационному обеспечению.

Функциональные требования

Функциональные требования предъявляются к:

1. Перечню защищаемой информации
2. Перечню угроз информационной системы (способы несанкционированного доступа к информации, несанкционированных и непреднамеренных воздействий на информацию в ИСиР)
3. Перечню подсистем информационного ресурса, участвующих в обработке защищаемой информации, в том числе к:
   - подсистеме управления доступом
   - подсистеме регистрации и учета
   - подсистеме обеспечения целостности
   - подсистеме антивирусной защиты
   - подсистеме управления информационной безопасностью
   - подсистеме резервного копирования, восстановления и архивирования
4. Требования по контролю функционирования системы защиты информации ИСиР.

Функциональные требования (2)

1. Требования к перечню защищаемой в ИСиР информации
   - Должен быть указан конкретный перечень в соответствии с утвержденным классификатором.
   - Определение конкретного перечня защищаемой информации должно осуществляться исходя из назначения ИСиР, целей защиты информации, состава и структуры ИСиР, а также состава и структуры подсистемы информационной безопасности. Перечень защищаемой информации определяется как для ИСиР в целом, так и для ее составных частей (компонентов).
2. Требования к перечню угроз
   - Оценка опасности возможных способов несанкционированного доступа к информации и несанкционированных воздействий на нее осуществляется по методикам, определенным в нормативных и методических документах ФСТЭК России и других ведомств, уполномоченных Правительством Российской Федерации на проведение соответствующих работ.
   - Перечень угроз определяется на предпроектной стадии сознания информационной системы
   - Определение (уточнение) перечня угроз возможно проводить на этапе технического проектирования подсистемы информационной безопасности.
3. Требования к перечню подсистем ИСиР, участвующих в обработке защищаемой информации
   - Должен быть указан конкретный перечень. В перечне должны быть описаны сегменты информационных сетей, включающих АРМ пользователей, а также сегменты информационных сетей, которые включают в себя серверы, предназначенные для обработки защищаемой информации.
   - Должны быть указаны сервисы, предоставляющие пользователям услуги по обработке защищаемой информации, и определены транспортные протоколы, используемые пользователями для доступа к защищаемой информации.

Функциональные требования (3)

4. Требования к подсистеме управления доступом:
   - Подсистема управления доступом должна обеспечивать защиту от НСД серверов, АРМ пользователей и прикладных сервисов. Кроме того, должна быть обеспечена защита от НСД аппаратно-программных средств, влияющих на функционирование сегментов информационных сетей, в которых обрабатывается защищаемая информация.
   - При создании подсистемы управления доступом могут использоваться как наложенные, так и встроенные в операционные системы и приложения системы защиты от НСД.
   - Доступ к защищаемым инфраструктурным и информационным ресурсам должен осуществляться в соответствии с матрицей доступа. При построении матрицы доступа:
     - для инфраструктурных ресурсов должна осуществляться идентификация терминалов, серверов, узлов сети, каналов связи, периферийных устройств - по логическим именам, адресам в информационной сети, уникальным кодам устройств, цифровым сертификатам и иным технологически допустимым параметрам;
     - для информационных ресурсов должна осуществляться идентификация сервисов, программ, томов, каталогов, файлов, записей, полей записей - по сетевым адресам доступа к ним, логическим именам, цифровым сертификатам и иным технологически допустимым параметрам;
     - пользователи идентифицируются по логическим именам, паролям, цифровым сертификатам, электронным ключам и иным параметрам.
     - Набор идентификаторов пользователя, необходимый для предоставления ему доступа к каждому отдельному инфраструктурному или информационному ресурсу, определяется на стадии технического проектирования подсистемы защиты информации и, как минимум, включает в себя логическое имя, пароль, цифровой сертификат или электронный ключ. Передача идентификационных параметров должна осуществляться по защищенному каналу связи.

Функциональные требования (4)

5. В **подсистеме регистрации и учета** должны регистрироваться события:

а) запуск и останов средств регистрации;

б) события, связанные со средствами безопасности, в том числе:

- любое использование программно-аппаратных средств аутентификации;
- принятие или отвержение любого используемого атрибута безопасности (например: пароля или цифрового сертификата) при аутентификации;
- отказ в создании нового сеанса с учетом ограничения на число одновременно устанавливаемых сеансов;
- все попытки установления сеансов пользователями;
- блокирование интерактивного сеанса механизмом его блокировки;
- успешное разблокирование интерактивного сеанса;
- окончание интерактивного сеанса механизмом его завершения;
- успешное применение предупредительных действий, которые должны использоваться при возможном нарушении безопасности;
- истечение срока действия атрибутов безопасности (паролей, цифровых сертификатов и пр.);
- получение разрешения на запрошенные операции;
- получение отказа на запрошенные операции;
- успешные и неуспешные попытки активизации (запуска) программ (процессов) субъектами доступа (пользователями);
- идентификатор пользователя или субъекта доступа неуспешно пытавшегося получить доступ к объекту доступа (сервису или файлу);
- любые попытки выполнения операций с системным журналом, т.е. любые попытки чтения, изменения или уничтожения системного журнала;
- извещения администратора в случае переполнения системного журнала.

Средства регистрации должны приписывать к каждой записи, по крайней мере, следующие данные:

- а) дату и время возникновения события, тип события, идентификатор субъекта доступа и результат завершения события: успешное/неуспешное;
- б) для каждого типа регистрируемого события с учетом специфики соответствующей функциональной компоненты другие характерные данные.

6. **Подсистема обеспечения целостности** обеспечивает целостность программных средств объекта защиты, а также неизменность программной среды. При этом:

- целостность объекта защиты проверяется при загрузке системы по контролируемым суммам компонент защиты;
- целостность программной среды обеспечивается как запретом на модификацию программ и конфигурационных файлов с помощью наложенных или встроенных в ОС средствами защиты от НСД, так и применением средств мониторинга событий информационной безопасности;
- должно проводиться периодическое тестирование функций защиты объекта защиты при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;
- должны быть в наличии средства восстановления объекта защиты, предусматривающие ведение двух копий программных средств защиты от НСД и их периодическое обновление и контроль работоспособности. Время восстановления критичных технических средств не должно превышать 12 часов, программных – 2 часа. Регламенты по восстановлению должны определять ответственных исполнителей (администраторов), средства и период времени, требуемый на восстановление.

7. Требования к **подсистеме антивирусной защиты**

- должны применяться только сертифицированные средства антивирусной защиты. **Установка и регулярное** обновление средств антивирусной защиты на автоматизированных рабочих местах и серверах АС должны осуществляться администраторами АС;
- должны быть разработаны и введены в действие **инструкции по антивирусной защите**, учитывающие особенности технологических процессов обработки информации комплексов городского хозяйства и территориального управления. Особое внимание должно быть уделено антивирусной фильтрации трафика электронного почтового обмена.
- отключение антивирусных средств не допускается. Установка и обновление антивирусных средств в организации должны контролироваться представителями подразделений (лицами) в организации, ответственными за обеспечение ИБ.
- должны быть разработаны организационно-технические меры, и введены в действие **инструкции по обеспечению режима безопасного функционирования** информационной системы в случае, когда невозможно обеспечить обновление сертифицированных средств антивирусной защиты.

8. Требования к **подсистеме управления информационной безопасностью**:

- должен быть определен порядок организации и выполнения работ по защите информации;
- должны быть определены должностные обязанности, права и степень ответственности сотрудников подразделения информационной безопасности;
- должны быть введены в эксплуатацию аппаратно-программные подсистемы управления подсистемой информационной безопасности;
- должен быть определен порядок физической защиты технических средств, образующих информационную систему, и осуществлены мероприятия по физической защите технических средств.

9. Требования к подсистеме резервного копирования, восстановления и архивирования:

- должны быть подготовлены регламенты по резервному копированию, восстановлению и архивированию с использованием специальных программно-аппаратных средств;
- процедуры резервного копирования, восстановления должны основываться на ведении циклически перезаписываемых нескольких (не менее трёх) наборов копий, в т.ч. территориально разнесенных;
- процедуры архивирования должны основываться на ведении нескольких (не менее двух) наборов копий;
- должно быть обеспечено территориальное разнесение архивных (страховочных) копий данных;
- временные характеристики функционирования подсистемы резервного копирования, восстановления и архивирования определяются на стадии технического проектирования, с обеспечением возможности создания как минимум ежедневного набора резервных копий.

10. Требования по **контролю функционирования** системы защиты информации ИСиР.

Контроль функционирования ПИБ должен обеспечиваться:

- силами собственного подразделения по защите информации (администратора безопасности);
- силами внешней эксплуатирующей организации;
- за счет подключения к системе мониторинга СоИБ;
- программно-техническим комплексом ПИБ.

Технические требования к компонентам ПИБ

Должны включать требования к следующим компонентам ПИБ, реализующим базовый уровень информационной безопасности:

- компонента защиты от НСД, управления доступом и регистрацией, в том числе при использовании средств телекоммуникаций
- компонента антивирусной защиты
- компонента систем хранения данных, резервного копирования и восстановления информации.
- компонента криптографической защиты информации и электронной цифровой подписи.

Варианты технических решений

Подсистемы	Технические средства	Варианты реализации
– управления доступом, в том числе при использовании средств телекоммуникаций; – регистрации и учета; – обеспечения целостности.	Программные средства разграничения доступа, регистрации и учета	Стандартное ПО в составе ОС, увязанное с TLS. ПО разграничения доступа.
	Аппаратные средства обеспечения целостности и защиты от НСД к РС и серверам	e-token, электронный замок
	Защита от внешних сетей – межсетевое экранирование	Стандартный МЭ в составе ОС, наложенный сертифицированный МЭ
	Защита от внешних сетей – средства обнаружения вторжений	SNORT, Real Secure, Форпост
	Защита от внешних сетей – сканеры защищенности	NESUS, ISS
	Средства криптографической защиты информации, в т.ч. клиентское программное обеспечение стандарта ЭЦП	СКЗИ «Крипто-ПРО», «Домен-К», пр.
	Средства хранения журнальных файлов и аудита безопасности	Стандартные средства ОС, модуль аудита, Система мониторинга СоИБ
антивирусной защиты	Средства антивирусной защиты	AVP, DoctorWeb, иные
резервного копирования, восстановления и архивирования	Программно-аппаратные средства резервного хранения	Backup средствами ОС, ЗЦРХД

Требования по нормативному обеспечению

- Организационно-распорядительные документы организации, составляющие ее политику информационной безопасности, должны включать:
  - меры по обеспечению информационной безопасности, включающие, в том числе:
    - порядок оформления, категорирования, предоставления доступа к информационным ресурсам ИСиР;
    - управление доступом к информационным системам, локальной и корпоративной сетям, приложениям и компьютерам;
    - требования по использованию паролей;
    - требования по защите оборудования, в том числе оборудования, оставляемого без присмотра;
    - требования по обеспечению антивирусной защиты;
    - требования к администрированию компьютерных систем и вычислительных сетей
    - правила работы с носителями информации и их защиты;
    - правила обмена данными и программами;
    - правила проведения аудита (контроля) состояния информационной безопасности объектов информатизации;
    - меры по обеспечению физической безопасности оборудования.
  - *правила представления информации, ведения делопроизводства и документооборота - КИ;*
  - *правила использования рабочего стола и персонального компьютера - КИ;*
  - *меры по обеспечению безопасности речевой информации - КИ*;

- Проектная документация на систему защиты информации должна включать следующие документы по информационной безопасности:
  - руководство пользователя;
  - руководство администратора СЗИ;
  - тестовая и инструктивно-методическая документация;
  - конструкторская (проектная) документация.

Требования по организационному обеспечению

- Требуется выполнение каждым обладателем (оператором) информационной системы следующих положений организационного обеспечения ИБ:
  - обеспечение штатного наполнения структуры ИБ;
  - определение порядка обращения с категорированной информацией в соответствии с требованиями нормативно-методических документов;
  - организация обеспечения контроля соответствия объектов информатизации требованиям безопасности информации.

- Для выполнения указанных требований должно быть обеспечено:
  - организация общей подготовки кадров организаций, предприятий и органов власти для выполнения установленных требований по обеспечению информационной безопасности;
  - организация подготовки специалистов для эксплуатации систем и средств защиты и обеспечения контроля соблюдения установленных требований к информационной безопасности в деятельности организаций, предприятий и органов власти;
  - получение письменного обязательства каждого, принимаемого на работу, сотрудника о соблюдении конфиденциальности. Условие соблюдения конфиденциальности должно распространяться на всю защищаемую информацию, доверенную сотруднику или ставшую ему известной в процессе выполнения им своих служебных обязанностей;
  - определены правила реагирования сотрудников на события, несущие угрозу безопасности;
  - вменены в обязанности сотрудникам обязательное уведомление об обнаруженных инцидентах и слабых местах в системе безопасности;
  - определена ответственность за нарушение режима безопасности информации.

Первоочередные мероприятия

- Проведение обследования (аудита) с целью выявления соответствия (не соответствия требованиям базового уровня безопасности)
- Формирование собственного организационно-технического плана мероприятий по достижению базового уровня безопасности и согласование его с уполномоченными органами власти
- Подача установленным порядком заявок на финансирование и подготовку/переподготовку кадров

- Спасибо за внимание

- И.Л.Дмитриев
- dmitriev@compusec.ru
- 917-0085