Некоммерческое Партнерство Специалистов Информационной Безопасности

Моделирование возможностей нарушителей в среде функционирования средств электронной подписи

Левиев Дмитрий Олегович

Некоммерческое Партнерство Специалистов Информационной Безопасности

Модель нарушителя КСИИ

- Лица сторонних организаций, осуществляющих строительство, оборудование, ремонт (модернизацию), текущее техническое обслуживание ОИ (строители, наладчики ОТСС, ВТСС, инженерного оборудования, средств обеспечения функционирования ОИ, технический персонал ОИ), или иные лица, легально находящиеся на территории ОИ по служебной необходимости
- Лица из состава персонала ОИ (организации, которой принадлежит ОИ), в том числе сотрудники охраны ОИ, не допущенные к информации, обсуждаемой в помещениях на территории ОИ

Некоммерческое Партнерство Специалистов Информационной Безопасности

Модель нарушителя КСИИ

- Лица нелегально оказавшиеся в пределах КЗ ОИ или в помещениях ОИ
- Лица из-за пределов КЗ ОИ, использующие средства дистанционной установки закладочных устройств
- Сотрудники ОИ (организации, которой принадлежит ОИ) как участвующими в совещаниях, переговорах в помещении, так и не участвующими в них
- Представители внешних организаций, участвующие в совещаниях, переговорах в помещении
- Представители внешних организаций, посетители, легально находящиеся на территории ОИ, но официально не допущенные к совещаниям, переговорам

Некоммерческое Партнерство Специалистов Информационной Безопасности

Модель нарушителя КСИИ

- Посторонние лица, нелегально проникшие на территорию ОИ
- Лица, осуществляющие строительство, оборудование, ремонт (модернизацию), текущее техническое обслуживание ОИ (строители, наладчики ОТСС, ВТСС, инженерного оборудования, средств обеспечения функционирования ОИ, технический персонал ОИ)
- Должностные лица (сотрудники) ОИ (организации, которой принадлежит ОИ), в том числе сотрудники охраны ОИ
- Представители внешних организаций, посетители, легально находящиеся на территории ОИ

Некоммерческое Партнерство Специалистов Информационной Безопасности

Модель нарушителя КСИИ

- Представители разведывательных служб иностранных государств
- Представители криминальных структур;
- Представители конкурентов (конкурирующих организаций);
- Недобросовестные партнеры;
- Посторонние лица
- Лица, имеющие санкционированный доступ в контролируемую зону, но не имеющие доступа к ИС
- Пользователи ИС, осуществляющие ограниченный доступ к ресурсам ИС с рабочего места

Некоммерческое Партнерство Специалистов Информационной Безопасности

Модель нарушителя КСИИ

- Зарегистрированные пользователи ИС, осуществляющий удаленный доступ к информации по ЛВС
- Зарегистрированные пользователи ИС с полномочиями администратора безопасности сегмента ИС
- Зарегистрированные пользователи с полномочиями системного администратора ИС
- Зарегистрированные пользователи с полномочиями администратора безопасности ИС
- Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте

Некоммерческое Партнерство Специалистов Информационной Безопасности

Модель нарушителя КСИИ

- Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на защищаемом объекте

Некоммерческое Партнерство Специалистов Информационной Безопасности

Модель нарушителя ПДн

- Разведывательные службы государств
- Криминальные структуры
- Конкуренты (конкурирующие организации)
- Недобросовестные партнеры
- Внешние субъекты (физические лица)
- Террорист

Некоммерческое Партнерство Специалистов Информационной Безопасности

Модель нарушителя ПДн

- Работник организации, имеющий санкционированный доступ к ИСПДн, но не имеющий доступа к ПДн.
- Зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.
- Зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам.
- Зарегистрированный пользователь ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн в пределах своей подсистемы ИСПДн.

Модель нарушителя ПДн

- Зарегистрированные пользователи с полномочиями системных администраторов
- Зарегистрированный пользователь с полномочиями администратора безопасности ИСПДн
- Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте
- Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн

Некоммерческое Партнерство Специалистов Информационной Безопасности

Модель нарушителя риск-ориентированный подход

- Экспертная оценка на 18.02.2013
- Модели классов актуальных угроз при проведении платежей с использованием систем ДБО

Некоммерческое Партнерство Специалистов Информационной Безопасности

Модель нарушителя риск-ориентированный подход

- Внешний злоумышленник
- Сотрудник компании клиента
- Клиент
- Сотрудник банка, обладающий законными правами, и третье лицо, не обладающее законными правами
- Сотрудник операционного подразделения Банка
- Внешний нарушитель

Модель нарушителя ЦБ (проект)

- Работники организации, реализующие угрозы безопасности ПДн с использованием легально предоставленных им полномочий в ИС
- Работники организации, реализующие угрозы безопасности ПДн вне легально предоставленных им полномочий в ИС
- Поставщики программно-технических средств, расходных материалов, услуг и подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования ИС и его ремонт

Некоммерческое Партнерство Специалистов Информационной Безопасности

Модель нарушителя ЦБ (проект)

- Криминальные элементы
- Компьютерные злоумышленники, осуществляющие несанкционированный доступ к ПДн или целенаправленное деструктивное воздействие на ПДн

Модель нарушителя ФСБ

- Н1 – внешний нарушитель
- Н2 – внутренний нарушитель, имеющий право доступа к помещение, но не имеющий право доступа к ИС
- Н3 – внутренний нарушитель, имеющий право легального доступа к ИС
- Н4 – внутренний нарушитель, одиночный специалист в области защиты информации, использующий и реализующий специальные методы атак
- Н5 – научно-исследовательские центры, специализирующиеся в области разработки и анализа СКЗИ
- Н6 – иностранные технические разведки

Некоммерческое Партнерство Специалистов Информационной Безопасности

Стандартные «допущения»

- Пользователь ИС является доверенным в рамках должностных/функциональных полномочий
- Администратор ИБ сегмента ИС доверенное лицо полностью или в рамках должностных/функциональных полномочий
- Системный администратор доверенное лицо
- Администратор ИБ доверенное лицо

Некоммерческое Партнерство Специалистов Информационной Безопасности

Варианты решения

- Согласование моделей нарушителей на уровне нормативно-правовой базы ФСБ России и ФСТЭК России
- Разработка методики соответствия моделей нарушителя с типовыми моделями нарушителя ФСТЭК России и ФСБ России
- Разработка риск-ориентированной модели нарушителя

Некоммерческое Партнерство Специалистов Информационной Безопасности

Вопросы

- Клуб http://forum.npsib.org
- leviev@npsib.org
- 8 (495) 971 8268
- 8 (926) 539 2667