Информационная безопасность банковских безналичных платежей. Часть 4 — Обзор стандартов моделирования угроз

В предыдущей публикации цикла мы сформировали базовые требования к системе информационной безопасности безналичных платежей и сказали, что конкретное содержание защитных мер будет зависеть от модели угроз.

Для формирования качественной модели угроз необходимо учесть существующие наработки и практики по данному вопросу.

В этой статье мы проведем экспресс обзор порядка 40 источников, описывающих процессы моделирования угроз и управления рисками информационной безопасности. Рассмотрим как ГОСТы и документы российских регуляторов (ФСТЭК России, ФСБ России, ЦБ РФ), так и международные практики.

Краткое описание процесса моделирования угроз

Конечным результатом процесса моделирования угроз должен стать документ – **модель угроз**, содержащий перечень значимых (актуальных) для защищаемого объекта угроз безопасности информации.

При моделировании угроз в качестве защищаемых объектов обычно рассматривают:

- информационные системы;
- автоматизированные системы;
- объекты информатизации;

- бизнес-процессы.

По большому счету модель угроз не обязательно должна быть представлена именно в виде перечня. Это может быть дерево (граф), майндкарта или какая-либо другая форма записи, позволяющая специалистам удобно с ней работать.

Конкретный состав угроз будет зависеть от свойств защищаемого объекта и реализуемых с его помощью бизнес-процессов. Соответственно одним из исходных данных для моделирования будет описание самого защищаемого объекта.

Если рассматривается некий гипотетический объект, то формируется **типовая (базовая) модель угроз**. Если рассматривается реальный объект, то формируется **частная модель угроз**.

При моделировании угроз, помимо описания защищаемого объекта, специалисты должны обладать знаниями о самих угрозах.

На практике эти знания можно почерпнуть из:
- отчетов исследователей об обнаруженных уязвимостях, которые могут быть использованы для реализации угроз;
- отчетов компьютерных криминалистов о расследованиях реальных компьютерных атак;
- отчетов компаний, специализирующихся в области защиты информации, посвященных анализу текущей ситуации в области компьютерной безопасности;
- публикаций в СМИ, посвященных компьютерным преступлениям;
- **банков данных** или **каталогов угроз**, в которых перечислены угрозы, сгруппированные по тому или иному принципу.

Первоначальным этапом процесса моделирования будет **идентификация угроз**, то есть подбор максимально большого перечня угроз, которые хотя бы теоретически могут воздействовать на защищаемый объект.

При реализации данного этапа природа играет со специалистами по информационной безопасности злую шутку. Проблема заключается в том, что человеческая память является ассоциативной, и мы не можем взять и извлечь из нее все содержимое, например, вспомнить все возможные угрозы.

Для того чтобы сформировать перечень всех возможных угроз, применяют различные ухищрения, позволяющие специалистам задавать себе определенные вопросы или использовать принципы, по которым угрозы будут извлекаться из памяти и записываться. Примерами таких техник могут быть **классификаторы угроз**, **деревья**

угроз или шаблоны типовых компьютерных атак. Об этих методах мы поговорим ниже.

После формирования перечня всех возможных угроз его начинают фильтровать, чтобы в конечном счете остались только значимые (актуальные) для организации угрозы. Процесс фильтрации, как правило, выполняется в несколько итераций, на каждой из которых отбрасываются угрозы по тому или иному признаку.

Начинают с **признака наличия возможностей** (ресурсов) у нарушителей для реализации угроз. Для его определения сначала формируют специальный документ – **модель нарушителя**, в котором выделяют вероятных нарушителей и определяют их возможности. Затем соотносят полученные ранее угрозы с моделью нарушителя и отбрасывают все угрозы, реализация которых выходит за рамки возможностей потенциальных нарушителей.

Следующим признаком для фильтрации угроз является **признак незначительности риска**. Вначале организация определяет уровень риска, который она считает незначительным. Затем оценивает риск от реализации каждой угрозы и, если он меньше или равен данному уровню, угрозу отбрасывают.

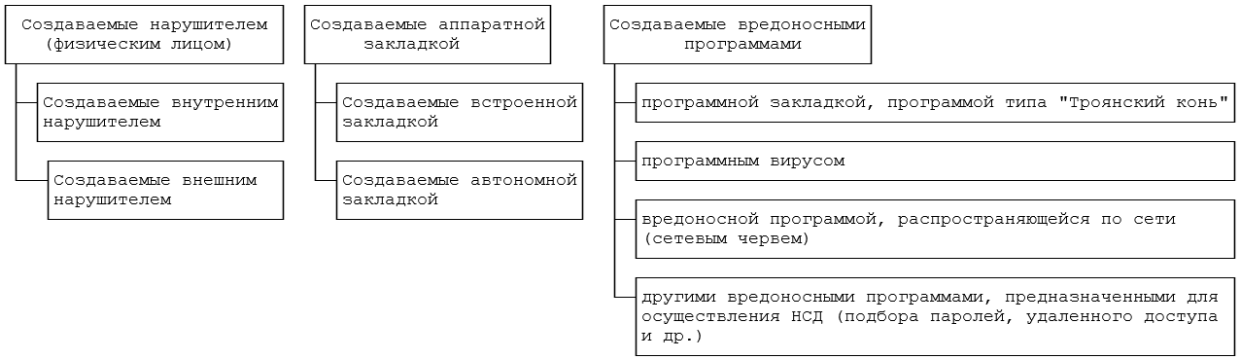
Таким образом, после окончания фильтрации будет получена модель угроз, содержащая значимые (актуальные) для организации угрозы безопасности информации.

Методика идентификации угроз – «классификаторы угроз»

Большинство угроз информационной безопасности можно сгруппировать (классифицировать) по тому или иному признаку. Полученные при этом классификационные схемы могут использоваться специалистами как вопросники к своей памяти, из которой они будут извлекать угрозы.

Возьмем, к примеру, задачу моделирования угроз безопасности персональных данных (ПДн), обрабатываемых в информационных системах персональных данных (ИСПДн).

ФСТЭК России в 2008 году выпустила для этих целей методический документ – Базовая модель угроз ПДн В данном документе содержится множество классификационных схем, из которых в качестве примера рассмотрим единственную — классификацию угроз по «источнику угрозу».



Специалист, строя частную модель угроз, может воспользоваться данной схемой, задать себе вопрос: «Какие угрозы персональным данным будут исходить от действий внутреннего нарушителя?» — и записать данные угрозы. Затем задать следующий вопрос: «А как внешний нарушитель может атаковать персональные данные?» и т. д. Подобная серия вопросов позволяет специалисту описать все известные ему угрозы, ни о чем не забыв.

Методика идентификации угроз – «дерево угроз»

При использовании данной методики специалист по информационной безопасности ставит себя на место нарушителя и начинает думать, как бы тот атаковал защищаемый объект.

В начале формулируется высокоуровневая угроза, которая будет являться корнем будущего дерева.

Затем специалист начинает декомпозировать данную угрозу на низкоуровневые, реализация которых может привести к реализации рассматриваемой угрозы. Для этого он может задаться вопросами, как или за счет чего исследуемая угроза может быть реализована.

Полученные при этом угрозы являются дочерними по отношению к рассматриваемой и записываются в дерево как ее потомки. Затем они, в свою очередь, также подвергаются декомпозиции, и так до достижения требуемого уровня детализации.

Подобный подход давно известен в технике и используется для построения деревьев неисправностей, формирование которых стандартизировано в ГОСТ Р 51901.13-2005 (МЭК 61025:1990) Менеджмент риска. Анализ дерева неисправностей.

Для иллюстрации использования «деревьев угроз» рассмотрим формирование модели угроз для объекта информатизации, представляющего собой изолированный, не подключенный к вычислительной сети компьютер. Предположим, что на данном

объекте обрабатывается важная информация, безопасность которой и требуется обеспечить.

В качестве высокоуровневой угрозы определим следующую: нарушение свойств защищенности охраняемой информации.

Общепринятыми свойствами защищенности являются конфиденциальность, целостность, доступность. Таким образом, дочерними угрозами будут:

- нарушение конфиденциальности защищаемых данных;
- нарушение целостности защищаемых данных;
- нарушение доступности защищаемых данных.

Декомпозируем угрозу «нарушение конфиденциальности защищаемых данных». Зададим себе вопрос: «За счет чего эта угроза может быть реализована?» — и в качестве ответа запишем следующие варианты:

- разглашение защищаемых данных со стороны лиц, допущенных к их обработке;
- осуществление несанкционированного доступа к защищаемым данным со стороны не допущенных лиц;
- утечка защищаемых данных по техническим каналам.

Аналогичным образом поступим с угрозой «нарушение целостности защищаемых данных». Она может быть декомпозирована на:

- повреждение защищаемых данных вследствие действий лиц, допущенных к их обработке;
- повреждение защищаемых данных вследствие действия вредоносного кода;
- повреждение защищаемых данных вследствие отказов и сбоев компьютера, на котором они обрабатываются.

Декомпозиция угрозы «нарушение доступности защищаемых данных» может быть представлена следующими угрозами:

- уничтожение защищаемых данных вследствие воздействия вредоносного кода (криптолокеры);
- уничтожение защищаемых данных вследствие выхода из строя жесткого диска компьютера, на котором они хранятся;
- нарушение условий эксплуатации объекта информатизации, делающее невозможным работу с ним персонала.

В итоге получим следующее дерево:

Как мы видим, даже такая примитивная модель, что мы только что построили, является довольно громоздкой при ее графическом отображении. Поэтому «деревья угроз» в основном документируются в виде иерархических списков.

Методика идентификации угроз «шаблоны типовых атак»

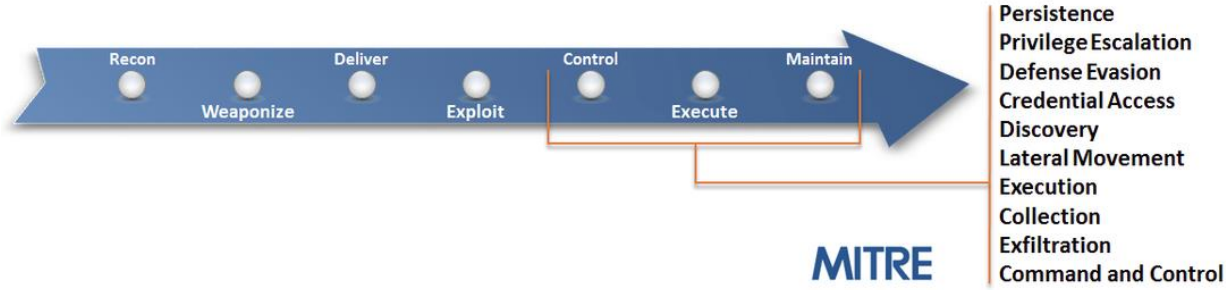
В основе данной методики лежит идея о том, что при осуществлении компьютерных атак злоумышленники всякий раз совершают некую схожую последовательность действий, которую можно назвать шаблоном типовой атаки.

Одним из наиболее известных на данный момент шаблонов компьютерных атак является описанный корпорацией Lockheed Martin шаблон kill chain, включающий в себя 7 этапов:

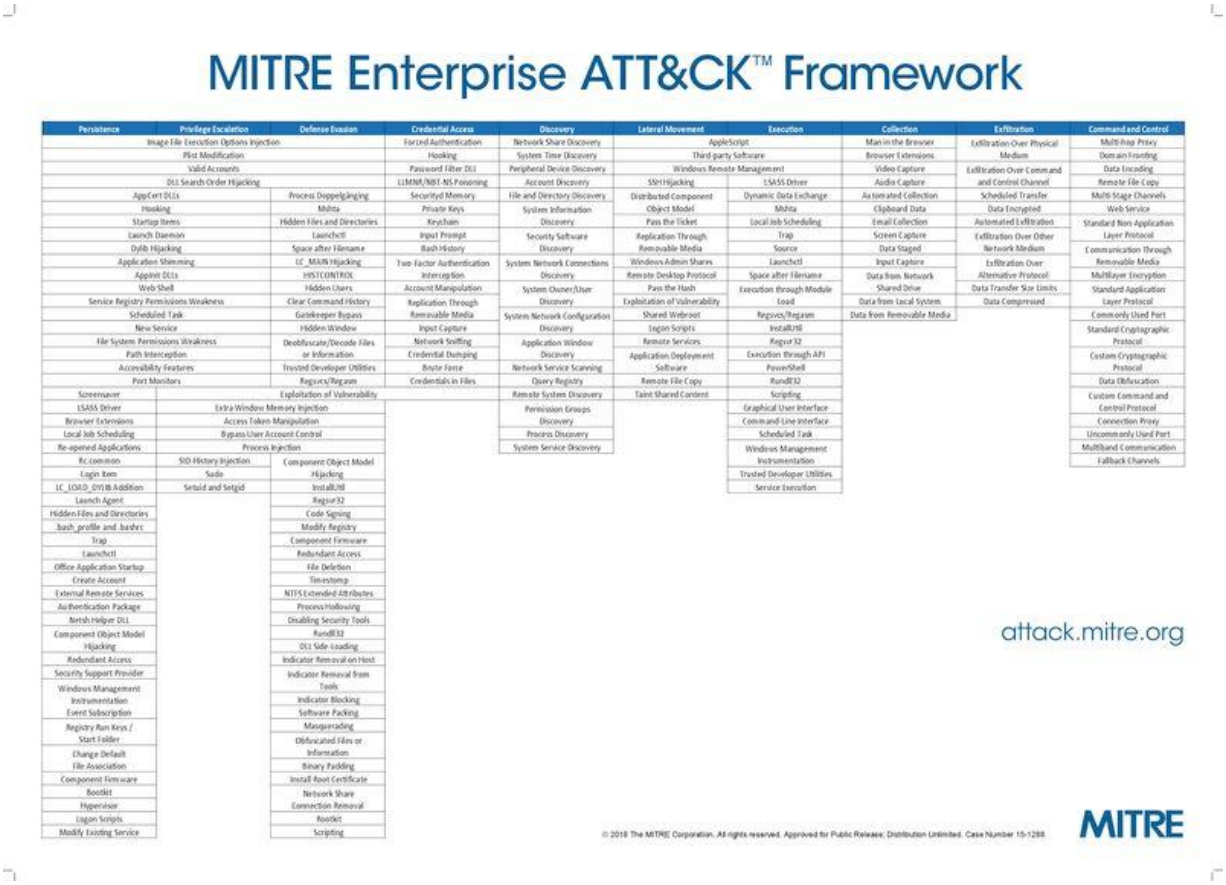
Этап 1. Разведка (Reconnaissance) – сбор данных об атакуемом объекте.

Этап 2. Разработка оружия (Weaponization) – разработка средств (вредоносного кода) для проведения атаки.
Этап 3. Доставка (Delivery) – доставка вредоносного кода на атакуемый объект.
Этап 4. Проникновение (Exploitation) – использование какой-либо уязвимости узла атакуемого объекта для запуска вредоносного кода.
Этап 5. Установка (Installation) – установка на скомпрометированный узел системы скрытого удаленного доступа.
Этап 6. Получение контроля (C2) – организация канала удаленного доступа злоумышленников к скомпрометированному узлу.
Этап 7. Действия (Actions) – совершение действий, ради которых и проводилась атака.

Научно-исследовательская организация MITRE, немного изменив наименования этапов, назвала данный шаблон – Cyber Attack Lifecycle.



Кроме того, MITRE расширила описание различных этапов и сформировала матрицу типовых тактик злоумышленников на каждом этапе. Данная матрица получила наименование ATT&CK.



(кликабельно)

Хотя приведенная матрица не является универсальной, она все же позволяет описать действия, предпринимаемые злоумышленниками при совершении большого числа реальных атак.

С точки зрения моделирования угроз шаблон типовой атаки может рассматриваться как классификатор угроз, а матрица типовых тактик — как значительный фрагмент модели угроз.

Уточнения будет требовать лишь последний этап шаблона – «Действия (Actions)», то, ради чего проводилась атака, ну и сами этапы могут быть дополнены не учтенными тактиками.

Документы ФСТЭК России по моделированию угроз персональным данным 2008 года.

1. Базовая модель угроз ПДн ФСТЭК, 2008 г.
2. Методика определения актуальных угроз ПДн 2008 г.

Оба документа являются методическими, то есть необязательными к применению, но

раскрывающими то, как по мнению ФСТЭК России должна решаться задача моделирования угроз безопасности ПДн.

Базовая модель угроз ПДн ФСТЭК, 2008 г. содержит единые исходные данные по угрозам безопасности ПДн, обрабатываемых в ИСПДн, связанным:

- с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

Задает формальное описание угроз:
- угроза утечки по техническим каналам := <источник угрозы>, < среда распространения ПДн и воздействий / приемник информативного сигнала / передатчик воздействующего сигнала>, <носитель ПДн>
- угроза НСД := <источник угрозы>, <уязвимость программного или аппаратного обеспечения>, <способ реализации угрозы>, <объект воздействия>, <несанкционированный доступ>.
- угроза НСД в ИСПДн: = <источник угрозы>, <уязвимость ИСПДн>, <способ реализации угрозы>, <объект воздействия (программа, протокол, данные и др.)>, <деструктивное действие>.
- угроза «Отказа в обслуживании»: = <источник угрозы>, <уязвимость ИСПДн>, <способ реализации угрозы>, <объект воздействия (носитель ПДн)>, <непосредственный результат реализации угрозы (переполнение буфера, блокирование процедуры обработки, «зацикливание» обработки и т.п.)>;
- угроза ПМВ в ИСПДн: = <класс вредоносной программы (с указанием среды обитания)>, <источник угрозы (носитель вредоносной программы)>, <способ инфицирования>, <объект воздействия (загрузочный сектор, файл и т.п.)>, <описание возможных деструктивных действий>, <дополнительная информация об угрозе (резидентность, скорость распространения, полиморфичность и др.)>.

При формальном описании угроз использовались следующие сокращения:
ИСПДн – информационная система персональных данных.
НСД – несанкционированный доступ.
ПМВ – программно-математическое воздействие (внедрение вредоносных программ).

В документе даны классификационные признаки угроз и уязвимостей, вредоносных программ. Предоставлен небольшой каталог типовых угроз, связанных с утечками по

техническим каналам и несанкционированным доступом. Приведена типовая модель нарушителей и определены их возможности.

Методика определения актуальных угроз ПДн 2008 г. определяет алгоритм, по которому можно провести фильтрацию угроз по признаку незначительности риска. Для этого в методике представлены способы определения возможности реализации угрозы (вероятности), показателя опасности угрозы (ущерба) и правила отнесения угрозы безопасности к не актуальным (обладающим незначительным риском).

Возможность реализации угрозы	Показатель опасности угрозы		
	низкая	средняя	высокая
Низкая	**неактуальная**	**неактуальная**	**актуальная**
Средняя	**неактуальная**	**актуальная**	**актуальная**
Высокая	**актуальная**	**актуальная**	**актуальная**
Очень высокая	**актуальная**	**актуальная**	**актуальная**

Документы ФСТЭК России по моделированию угроз в государственных информационных системах (ГИС) и банк данных угроз ФСТЭК России.

1. Методический документ ФСТЭК России. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014 г.)
2. Проект методического документа ФСТЭК России. Методика определения угроз безопасности информации в информационных системах
3. Банк данных угроз ФСТЭК России (bdu.fstec.ru).

Методический документ ФСТЭК России. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014 г.). Угрозы безопасности информации (УБИ) определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

Формальное описание угрозы безопасности информации:
УБИ: = [возможности нарушителя; уязвимости информационной системы; способ реализации угрозы; последствия от реализации угрозы].

Возможности (потенциал) нарушителей разделяют на три группы:
1. Нарушитель с базовым потенциалом.

2. Нарушитель с базовым усиленным потенциалом
3. Нарушитель с высоким потенциалом

Расшифровка возможностей нарушителей приведена в проекте методического документа ФСТЭК России. Методика определения угроз безопасности информации в информационных системах.

Описание и классификация уязвимостей происходит с применением национальных стандартов:

- ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей
- ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем

Сами уязвимости, способы реализации угроз и возможный ущерб приведены в банке данных угроз ФСТЭК России.

Методические рекомендации ФСБ России по моделированию угроз безопасности персональных данных

1. «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (утв. ФСБ России 31.03.2015 N 149/7/2/6-432).

Методические рекомендации определяют основные угрозы ПДн, которые могут быть нейтрализованы только с помощью СКЗИ. К ним относятся:
1. передача персональных данных по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче персональных данных по информационно-телекоммуникационным сетям общего пользования);
2. хранение персональных данных на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

Также в документе определена классификация возможностей нарушителей:

N	Обобщенные возможности источников атак
1	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны

N	Обобщенные возможности источников атак
2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее — АС), на которых реализованы СКЗИ и среда их функционирования
3	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования
4	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)
5	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)
6	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)

Документы Банка России о рисках информационной безопасности

1. Письмо ЦБ РФ от 7 декабря 2007 г. № 197-Т “О рисках при дистанционном банковском обслуживании”
2. Указание Банка России от 10 декабря 2015 г. № 3889-У «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных”
3. Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009. «Методика оценки рисков нарушения информационной безопасности»

Письмо ЦБ РФ от 7 декабря 2007 г. № 197-Т “О рисках при дистанционном банковском обслуживании” содержит перечень типовых угроз системам дистанционного банковского обслуживания и их клиентам, включая:

- Осуществление DoS/DDoS атак в отношении серверов ДБО.
- Кража персональной информации клиентов банка за счет фишинга через электронную почту.
- Кражи реквизитов платежных карт при помощи скиминговый атак и фальшивых банкоматов.
- Кража реквизитов доступа клиентов к системам ДБО при помощи социальной инженерии и телефонного мошенничества.

Указание Банка России от 10 декабря 2015 г. № 3889-У „Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных

в информационных системах персональных данных" содержит отраслевой перечень угроз безопасности персональным данным, включающий следующие угрозы:

- угроза несанкционированного доступа к персональным данным лицами, обладающими полномочиями в информационной системе персональных данных, в том числе в ходе создания, эксплуатации, технического обслуживания и (или) ремонта, модернизации, снятия с эксплуатации информационной системы персональных данных;
- угроза воздействия вредоносного кода, внешнего по отношению к информационной системе персональных данных;
- угроза использования методов социального инжиниринга к лицам, обладающим полномочиями в информационной системе персональных данных;
- угроза несанкционированного доступа к отчуждаемым носителям персональных данных;
- угроза утраты (потери) носителей персональных данных, включая переносные персональные компьютеры пользователей информационной системы персональных данных;
- угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в организации защиты персональных данных;
- угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в программном обеспечении информационной системы персональных данных;
- угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных;
- угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационной системы персональных данных;
- угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств криптографической защиты информации.

Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009. «Методика оценки рисков нарушения информационной безопасности»

Документ предлагает следующие процедуры оценки рисков:
Процедура 1. Определение перечня типов информационных активов, для которых

выполняются процедуры оценки рисков нарушения ИБ (далее — область оценки рисков нарушения ИБ).

Процедура 2. Определение перечня типов объектов среды, соответствующих каждому из типов информационных активов области оценки рисков нарушения ИБ.

Процедура 3. Определение источников угроз для каждого из типов объектов среды, определенных в рамках выполнения процедуры 2.

Процедура 4. Определение СВР угроз ИБ применительно к типам объектов среды, определенных в рамках выполнения процедуры 2.3.

Процедура 5. Определение СТП нарушения ИБ для типов информационных активов области оценки рисков нарушения ИБ.

Процедура 6. Оценка рисков нарушения ИБ.

Степень допустимости риска предлагается оценивать по «классической» таблице оценке рисков, учитывающей вероятность и возможный ущерб.

СВР угроз ИБ	СТП нарушения ИБ			
	минимальная	**средняя**	**высокая**	**критическая**
нереализуемая	допустимый	допустимый	допустимый	допустимый
минимальная	допустимый	допустимый	допустимый	недопустимый
средняя	допустимый	допустимый	недопустимый	недопустимый
высокая	допустимый	недопустимый	недопустимый	недопустимый
критическая	недопустимый	недопустимый	недопустимый	недопустимый

Здесь СВР – степень возможности реализации угрозы, СТП – степень тяжести последствий

Рекомендации также содержат небольшой каталог угроз, разбитых по классам.

Класс 1. Источники угроз ИБ, связанные с неблагоприятными событиями природного, техногенного и социального характера.

Класс 2. Источники угроз ИБ, связанные с деятельностью террористов и лиц, совершающих преступления и правонарушения.

Класс 3. Источники угроз ИБ, связанные с деятельностью поставщиков/провайдеров/партнеров.

Класс 4. Источники угроз ИБ, связанные со сбоями, отказами, разрушениями/повреждениями программных и технических средств.

Класс 5. Источники угроз ИБ, связанные с деятельностью внутренних нарушителей ИБ.

Класс 6. Источники угроз ИБ, связанные с деятельностью внешних нарушителей ИБ.

Класс 7. Источники угроз ИБ, связанные с несоответствием требованиям надзорных и регулирующих органов, действующему законодательству.

Национальные стандарты Российской Федерации (ГОСТы)

1. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения
2. ГОСТ Р ИСО/ТО 13569-2007. Финансовые услуги. Рекомендации по информационной безопасности
3. ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей
4. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем
5. ГОСТ Р 53113.1-2008 Информационная технология (ИТ). Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения
6. ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения
7. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

Данный ГОСТ идеологически связан с ГОСТ Р 50922-2006 Защита информации. Основные термины и определения, методическим документом «Специальные требования и рекомендации по защите конфиденциальной информации (СТР-К)» (ДСП) и действующими документами по аттестации объектов информатизации. Документ содержит в себе классификацию факторов, воздействующих на информацию, которую можно интерпретировать как угрозы информационной безопасности.

ГОСТ Р ИСО/ТО 13569-2007. Финансовые услуги. Рекомендации по информационной безопасности

Приложение «С» данного стандарта содержит в себе пример оценки рисков информационной безопасности для кредитно-финансовой организации. Для этого предлагается проводить анализ среди основных объектов вредоносных воздействий, включающих в себя персонал, аппаратуру, бизнес приложения, системы связи, программные средства и операционные системы. Ущерб от рисков оценивается в виде финансовых убытков, уменьшения продуктивности, ущерб репутации и как итоговый ущерб.

Уязвимости	Категория риска			
	Финансовые убытки	Уменьшение продуктивности	Ущерб для репутации	Общий риск
Персонал				
Аппаратура и оборудование				
Приложения				
Системы связи				
Программные средства среды и операционные системы				

ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей и ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем служат для описания уязвимостей информационных систем. Стандарты применяются совместно с основополагающим ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

В стандартах приведена классификация уязвимостей информационных систем, содержащая три классификационных признака:

1. по области происхождения;
2. по типам недостатков ИС;
3. по месту возникновения (проявления).

Сами уязвимости предлагается описывать в виде паспорта, содержащего следующие разделы:

1. Наименование уязвимости.
2. Идентификатор уязвимости.
3. Идентификаторы других систем описаний уязвимостей.
4. Краткое описание уязвимости.
5. Класс уязвимости.
6. Наименование ПО и его версия.
7. Служба (порт), которая (который) используется для функционирования ПО.
8. Язык программирования ПО.
9. Тип недостатка.
10. Место возникновения (проявления) уязвимости.
11. Идентификатор типа недостатка.
12. Наименование операционной системы и тип аппаратной платформы.
13. Дата выявления уязвимости.

14. Автор, опубликовавший информацию о выявленной уязвимости.
15. Способ (правило) обнаружения уязвимости.

В качестве языка правил обнаружения уязвимостей стандарты предлагают использовать OVAL.

ГОСТ Р 53113.1-2008 Информационная технология (ИТ). Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения

В стандарте описываются угрозы, связанные со скрытыми каналами, которые определяются как непредусмотренные разработчиком системы информационных технологий и автоматизированных систем коммуникационные каналы, которые могут быть применены для нарушения политики безопасности.

Угроза	Тип скрытых каналов	
	Скрытые каналы с низкой пропускной способностью	Скрытые каналы с высокой пропускной способностью
Внедрение вредоносных программ и данных	+	+
Подача злоумышленником команд агенту для выполнения	+	+
Утечка криптографических ключей или паролей	+	+
Утечка отдельных информационных объектов	-	+
Примечание - знак "+" - означает, что имеется связь угрозы с соответствующим типом скрытого канала; знак "-" - означает, что связи не существует.		

ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения

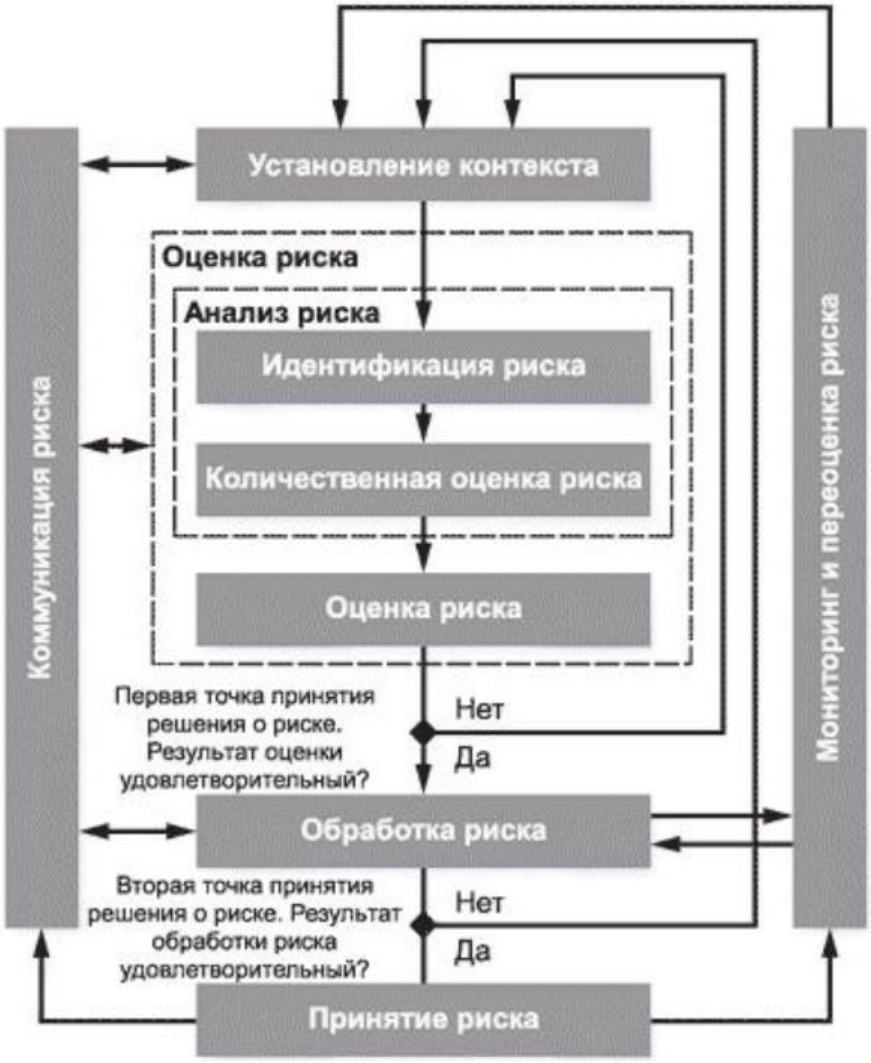
Данный документ является методическим документом для операторов связи, содержит общую схему действий по защите сетей связи:

В основе процесса моделирования угроз предлагается использовать ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. В стандарте приведена модель предполагаемых нарушителей.

Отличительной особенностью данного документа является то, что кроме классических свойств безопасности информации, таких как конфиденциальность, целостность, доступность, стандарт рассматривает также и подотчетность.

Под подотчетностью стандарт определяет свойство, которое обеспечивает однозначное отслеживание действий в сети любого объекта. Нарушение подотчетности — отрицание действий в сети (например, участие в совершенном сеансе связи) или подделка (например, создание информации и претензии, которые якобы были получены от другого объекта или посланы другому объекту).

ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности
Данный стандарт является частью группы стандартов обеспечения информационной безопасности, которые часто называют ISO 27K. В документе основной упор сделан на процедуры менеджмента при управлении рисками информационной безопасности.



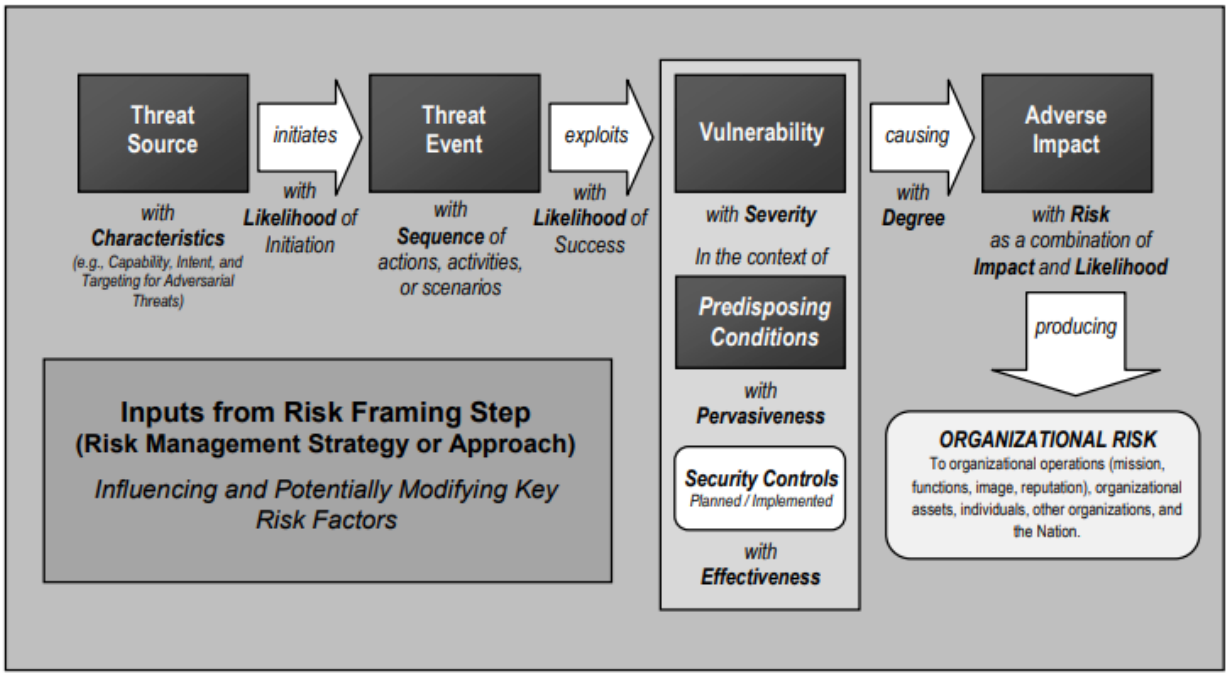
В приложении «C» приведены примеры типовых угроз, а в приложении «D» представлены типовые уязвимости.

Специальные публикации NIST

1. NIST SP 800-30. Guide for Conducting Risk Assessments
2. NIST SP 800-39. Managing Information Security Risk

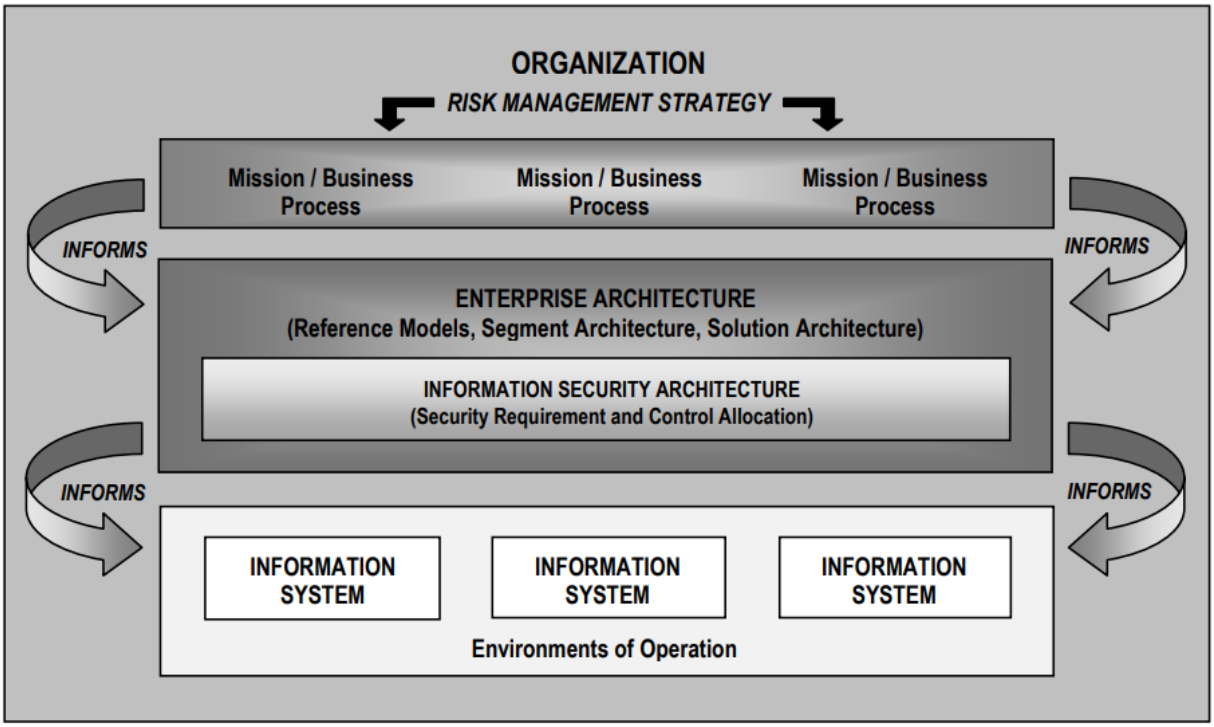
NIST SP 800-30. Guide for Conducting Risk Assessments

Документ ориентирован на вопросы управления рисками уровня менеджмента организации.



NIST SP 800-39. Managing Information Security Risk

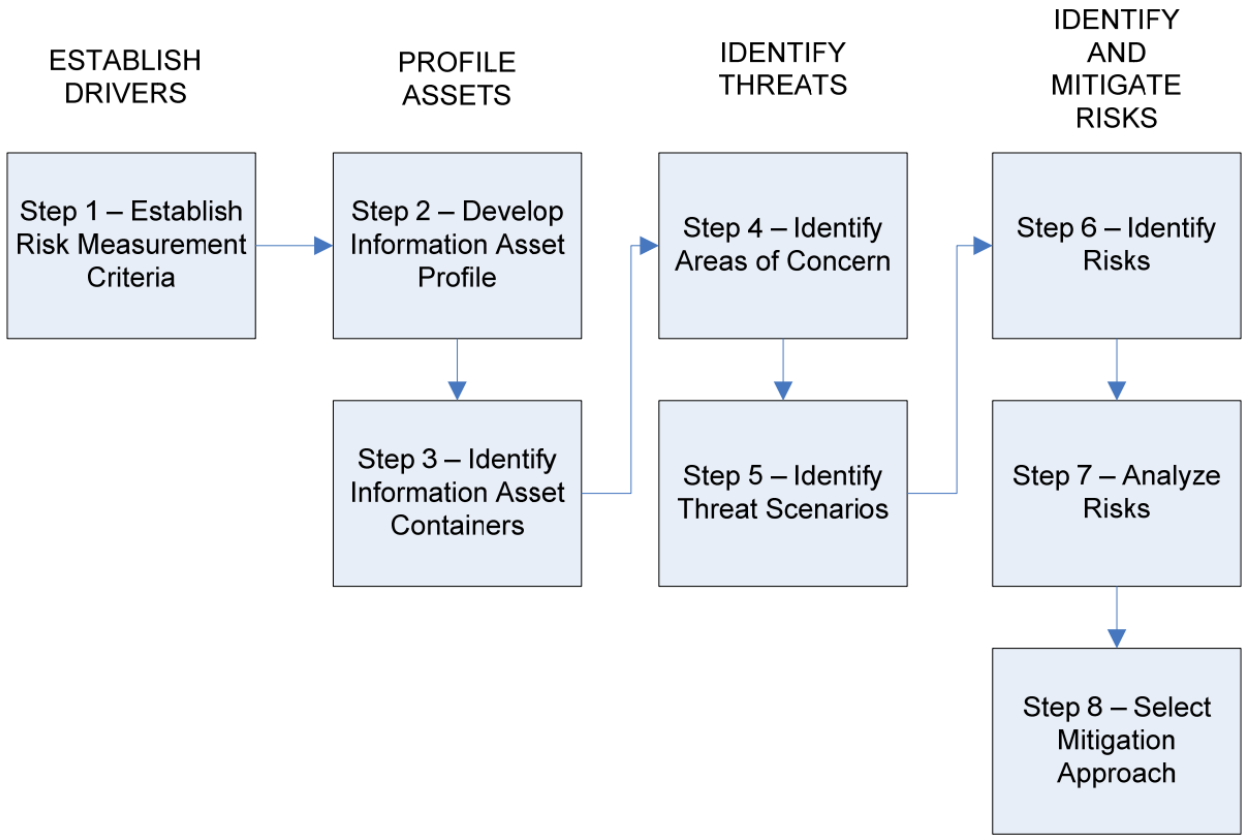
Документ описывает методологию управления рисками информационной безопасности уровня предприятия. Основная цель методологии связать систему информационной безопасности с миссией и целями организации



OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

OCTAVE методология управления рисками информационной безопасности, основной целью которой является обеспечение соответствия целей процессов защиты

информации целям и задачам, стоящим перед организацией. Методология состоит из 8 основных шагов:



1. Определение критериев измерения рисков (Establish Risk Measurement Criteria).
2. Разработка профилей информационных активов (Develop an Information Asset Profile).
3. Идентификация мест хранения / обработки / передачи информационных активов (Identify Information Asset Containers).
4. Выделение групп высокоуровневых угроз информационной безопасности (Identify Areas of Concern)
5. Идентификация угроз информационной безопасности (Identify Threat Scenarios)
6. Идентификация рисков информационной безопасности (Identify Risks)
7. Анализ рисков информационной безопасности (Analyze Risks)
8. Выбор мер обработки рисков информационной безопасности (Select Mitigation Approach)

Для идентификации угроз, осуществляемой на шаге 5, используется методология «дерева угроз».

Методология Trike

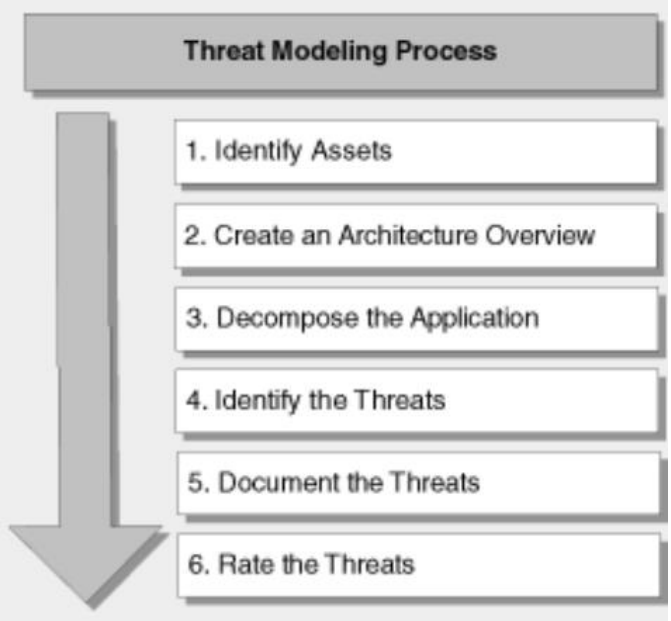
Trike основана на риск-ориентированном подходе к построению информационной безопасности и предназначена для проведения аудитов информационной безопасности и построения моделей угроз.

Отличительными особенностями данной методологии являются:

- ее изначальная ориентация на использование специализированного ПО для построения моделей угроз;
- использование «деревьев атак» для описания угроз безопасности;
- использование библиотек типовых атак.

Методики и публикации Microsoft по моделированию угроз

Для разработки безопасного ПО компания Microsoft применяет методологию Security Development Lifecycle. Данная методология представляет собой расширение к «классической» – каскадной модели разработки ПО («waterfall»), в которую вносятся дополнительные этапы, связанные с обеспечением безопасности. На этапе «Дизайн (design)» предлагается проводить моделирование угроз.



Для идентификации угроз предлагается использовать несколько подходов:

- методология STRIDE;
- использование классификаторов угроз;
- использование деревьев угроз и шаблонов атак.

Методология STRIDE представляет собой классификационную схему для описания атак в зависимости от типа используемых для их реализации эксплойтов или мотивации нарушителя.

STRIDE – это акроним от первых букв:

- **S**poofing Identity – «подмена личности». Нарушитель выдает себя за легитимного пользователя (например, украл логин/пароль) и выполняет от его имени вредоносные действия.
- **T**ampering with Data – «подделка данных». Нарушитель подделывает данные, которые ему доступны при работе Web-приложения. Это могут быть cookie, элементы HTTP-запросов и т.д.
- **R**epudiation – «отказ от транзакций». Нарушитель может отказаться от транзакций, когда на стороне Web-приложения не ведется достаточный аудит действий пользователей.
- **I**nformation Disclosure – «раскрытие чувствительной информации». Нарушитель старается раскрыть персональные данные других пользователей, аутентификационную информацию и т.д.
- **D**enial of Service – «отказ в обслуживании».
- **E**levation of Privilege – «повышение привилегий».

После идентификации угроз SDL предлагает оценить порождаемые ими риски. Для этого может использоваться методика DREAD.

Название методики DREAD так же является акронимом от первых букв категорий, по которым оценивается риск:

- **D**amage Potential – какой ущерб будет нанесен, если угроза реализуется?
- **R**eproducibility – насколько просто реализовать угрозу?
- **E**xploitability – что требуется для того, чтобы выполнить атаку?
- **A**ffected Users – сколько пользователей может пострадать от атаки?
- **D**iscoverability – насколько просто злоумышленник может обнаружить угрозу?

Сам риск оценивается по формуле:

Risk_DREAD = (DAMAGE + REPRODUCIBILITY + EXPLOITABILITY + AFFECTED USERS + DISCOVERABILITY) / 5,

где значение составных элементов варьируется от 0 до 10. Например, значение Damage Potential может определяться как:

- 0 = ущерба не будет;
- 5 = ущерб будет лишь некоторой части системы или ограниченному объему данных;
- 10 = пострадает вся система или будут уничтожены все данные.

Каталоги угроз

1. OWASP Top10

Содержит описание основных угроз Web-приложениям.

2. OWASP Testing project

Содержит рекомендации по тестированию безопасности Web-приложений.

3. WASC Threat Classification

Еще один источник, содержащий описание типовых атак на Web-приложения.

4. Bluetooth Threat Taxonomy

Содержит данные по уязвимостям протокола Bluetooth.

5. ENISA Threat Landscape

Ежегодный отчет агентства по кибербезопасности Евросоюза, содержащий сведения об основных угрозах.

6. ENISA Threat Taxonomy

Еще один документ агентства по кибербезопасности ЕС, содержащий классификацию и описание основных угроз информационной безопасности.

7. BSI Threat catalogue

Каталог федерального агентства по информационной безопасности Германии, содержащий описание преимущественно угроз физического уровня (пожаров, краж, ионизирующей радиации и т. д.).

8. Open Threat Taxonomy

Проект с открытым исходным кодом, включающий в себя ПО и различные классификационные схемы в JSON формате, используемые для обмена данными об угрозах информационной безопасности.

9. US DoD Comprehensive Military Unmanned Aerial Vehicle smart device ground control station threat model

Документ Министерства обороны США, содержащий модель угроз наземным станциям управления беспилотными летательными аппаратами.

10. VoIP Security and Privacy Threat Taxonomy

Документ, содержащий описание угроз VoIP.

11. Mobile Threat Catalogue

Информационный ресурс NIST, включающий в себя обширный каталог угроз, связанных с применением мобильных устройств и технологий.

12. ATT&CK

Матрица техник и тактик, применяемых реальными нарушителями при взломах информационных систем.

13. Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009. «Методика оценки рисков нарушения информационной безопасности»

Документ Банка России по управлению рисками, содержащий в приложении описание типовых угроз.

14. Банк данных угроз безопасности информации ФСТЭК России

Основной каталог угроз и уязвимостей ФСТЭК России. Используется для моделирования угроз в государственных и муниципальных информационных системах.

15. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

Стандарт, описывающих типовые угрозы информационной безопасности. Большое внимание уделено угрозам, связанным с утечками информации по техническим каналам.

16. Базовая модель угроз ПДн ФСТЭК, 2008 г.

Документ ФСТЭК России, содержащий классификационные схемы типовых угроз безопасности персональных данных, а также описание небольшого числа наиболее вероятных угроз.