Программно-аппаратная защита

Лекция на тему: «Модели безопасности защиты от несанкционированного доступа»

ФИО преподавателя: Оцоков Ш.А.

2021

ГОСТ Р ИСО/МЭК 17799:2005

МИРЭА
Российский технологический университет

ГОСТ Р ИСО/МЭК 17799:2005 «Информационная технология. Практические правила управления информационной безопасностью»

Кратко перечислим разделы стандарта и предлагаемые в них мероприятия по защите информации. Первая их группа касается политики безопасности. Требуется, чтобы она была разработана, утверждена руководством организации, издана и доведена до сведения всех сотрудников. Она должна определять порядок работы с информационными ресурсами организации, обязанности и ответственность сотрудников. Политика периодически пересматривается, чтобы соответствовать текущему состоянию системы и выявленным рискам.

Следующий раздел затрагивает организационные вопросы, связанные с обеспечением информационной безопасности.

Данный стандарт рассматривает вопросы информационной безопасности, в том числе,

и с точки зрения экономического эффекта, включая оценку рисков

ГОСТ Р ИСО/МЭК 17799:2005

При предоставлении доступа к информационным системам специалистам сторонних организаций необходимо особое внимание уделить вопросам безопасности. Должна быть проведена оценка рисков, связанных с разными типами доступа (физическим или логическим, т. е. удаленным) таких специалистов к различным ресурсам организации.

Следующий раздел стандарта посвящен вопросам классификации и управления активами. Для обеспечения информационной безопасности организации необходимо, чтобы все основные информационные активы были учтены и закреплены за ответственными владель цами. Начать предлагается с проведения инвентаризации, например:

- информационные (базы данных и файлы данных, системная до кументация и т. д.);
- программное обеспечение (прикладное программное обеспечение, системное программное обеспечение, инструментальные средства разработки и утилиты);
- физические активы (компьютерное оборудование, оборудование связи, носители информации, другое техническое оборудование, мебель, помещения);
- услуги (вычислительные услуги и услуги связи, основные коммунальные услуги).

ГОСТ Р ИСО/МЭК 17799:2005

Далее предлагается классифицировать информацию, чтобы определить ее приоритетность, необходимость и степень ее защиты. При этом можно оценить соответствующую информацию с учетом того, насколько она критична для организации, например, с точки зрения обеспечения ее целостности и доступности. После этого предлагается разработать и внедрить процедуру маркировки при обработке информации.

Подводя итог можно отметить, что в стандарте рассмотрен широкий круг вопросов, связанных с обеспечением безопасности информационных систем, и по ряду направлений даются практические рекомендации.

ГОСТ Р ИСО/МЭК 27001-2006

МИРЭА Российский технологический университет

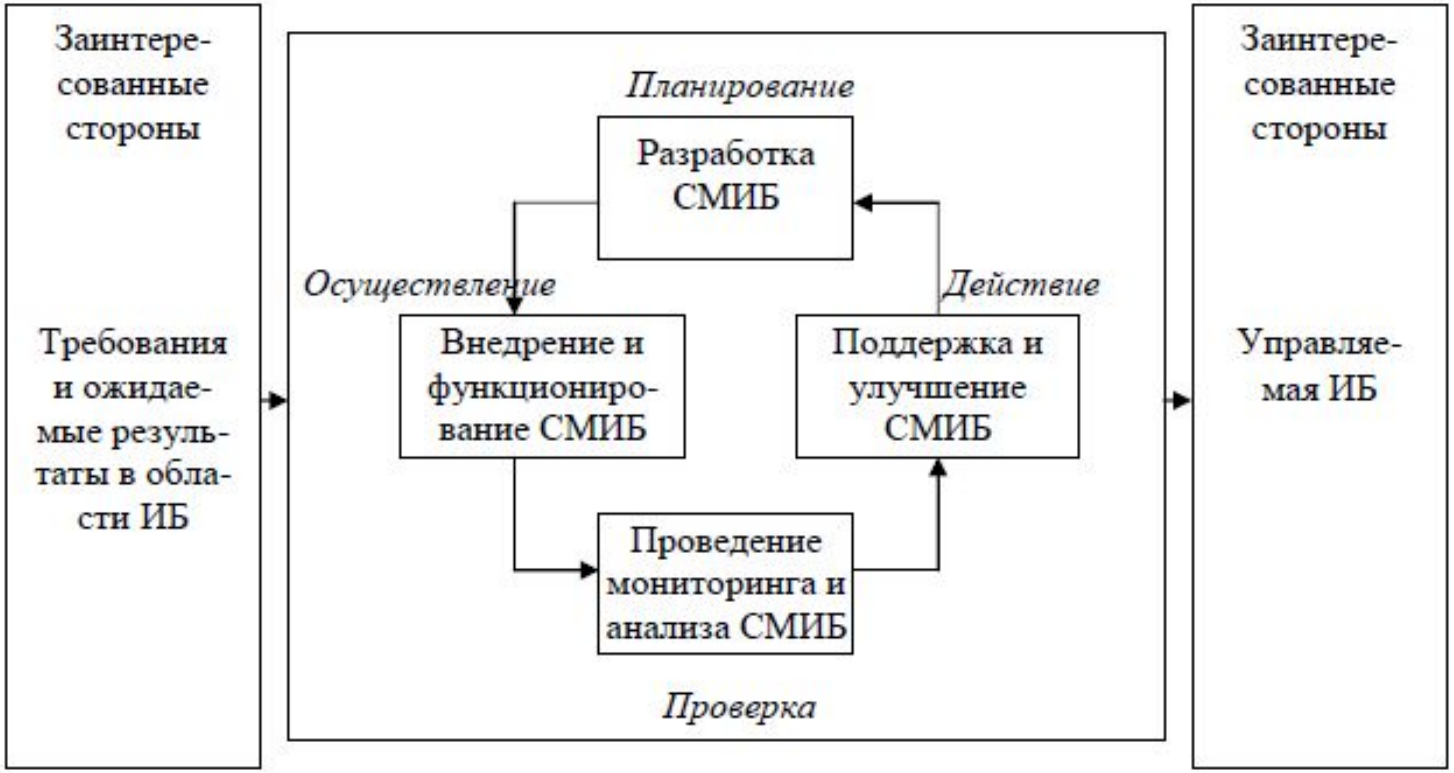
ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»

Разработчики стандарта отмечают, что он был подготовлен в качестве модели для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы менеджмента информационной безопасности (СМИБ). СМИБ (англ. — information security management system; ISMS) определяется как часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности. Система менеджмента включает в себя организационную структуру, политики, деятельность по планированию, распределение ответственности, практическую деятельность, процедуры, процессы и ресурсы.

Стандарт предполагает использование процессного подхода для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СМИБ организации. Он основан на модели «Планирование (Plan) – Осуществление (Do) – Проверка (Check) – Действие (Act)» (PDCA), которая может быть применена при структурировании всех процессов СМИБ.

ГОСТ Р ИСО/МЭК 27001-2006

Этапы построения и использования СМИБ [1]



ГОСТ Р ИСО/МЭК 27001-2006

организация должна в соответствии с утвержденным графиком проводить внутренние аудиты СМИБ, позволяющие оценить ее функциональность и соответствие стандарту. А руководство должно проводить анализ системы менеджмента информационной безопасности.
Также должны проводиться работы по улучшению системы менеджмента информационной безопасности: повышению ее результативности и уровня соответствия текущего состояния системы и предъявляемым к ней требованиям.
В приложении к стандарту перечисляются рекомендуемые меры управления, взятые из ранее рассмотренного стандарта ISO/IEC 17799:2005.

Политика безопасности

МИРЭА Российский технологический университет

Вопросы защиты информации в АС регламентируется политикой безопасности. **Политика безопасности** определяется как совокупность документированных управленческих решений направленных на защиту информации и ассоциированных с ней ресурсов.

Основная цель политики безопасности это информирование пользователей сотрудников и руководства о наложенных на них обязательных требованиях по защите технологии информационных ресурсов

1. Невозможность миновать защитное средство
2. Усиление слабого звена
3. Недопустимость перехода в открытое состояние
4. Минимизация привилегии
5. Разделение обязанностей
6. Многоуровневая защита
7. Разнообразие защитных средств
8. Простота и управляемость информационной системы

Политика безопасности

МИРЭА Российский технологический университет

- определение целей политики безопасности
- определение принципов обеспечения границ применимости политики безопасности
- Краткое разъяснение политики безопасности
- соответствие законодательным актам и стандартам
- определение правил приобретения информационных технологий, которые отвечает требования безопасности
- определение политики обеспечения непрерывной работы
- определение политики конфиденциальности стандартных сервисов
- определение политики аутентификации
- определение политики разграничения доступа
- обнаружение блокирование вирусов
- определение о порядке разработки и сопровождения автоматизированных систем
- обучение персонала вопросам защиты информации
- защита от недекларированных возможностей ПО
- аудит и обновление политики безопасности

Одновременно создается специальное штатное подразделение одно или несколько должностных лиц органа обеспечения безопасности информации

Политика безопасности

МИРЭА
Российский технологический университет

Классифицирование

Двух или трех уровней классификации обычно достаточно для любой организации. Самый нижний уровень классификации - это общая информация. Над этим уровнем находится информация, недоступная для общего пользования. Она называется проприетарной, секретной или конфиденциальной.

Существует третий уровень секретности, который называется "для служебного пользования" или "защищенная *информация*". *Доступ* к подобным сведениям открыт для ограниченного количества служащих.

Маркировка и хранение секретной информации

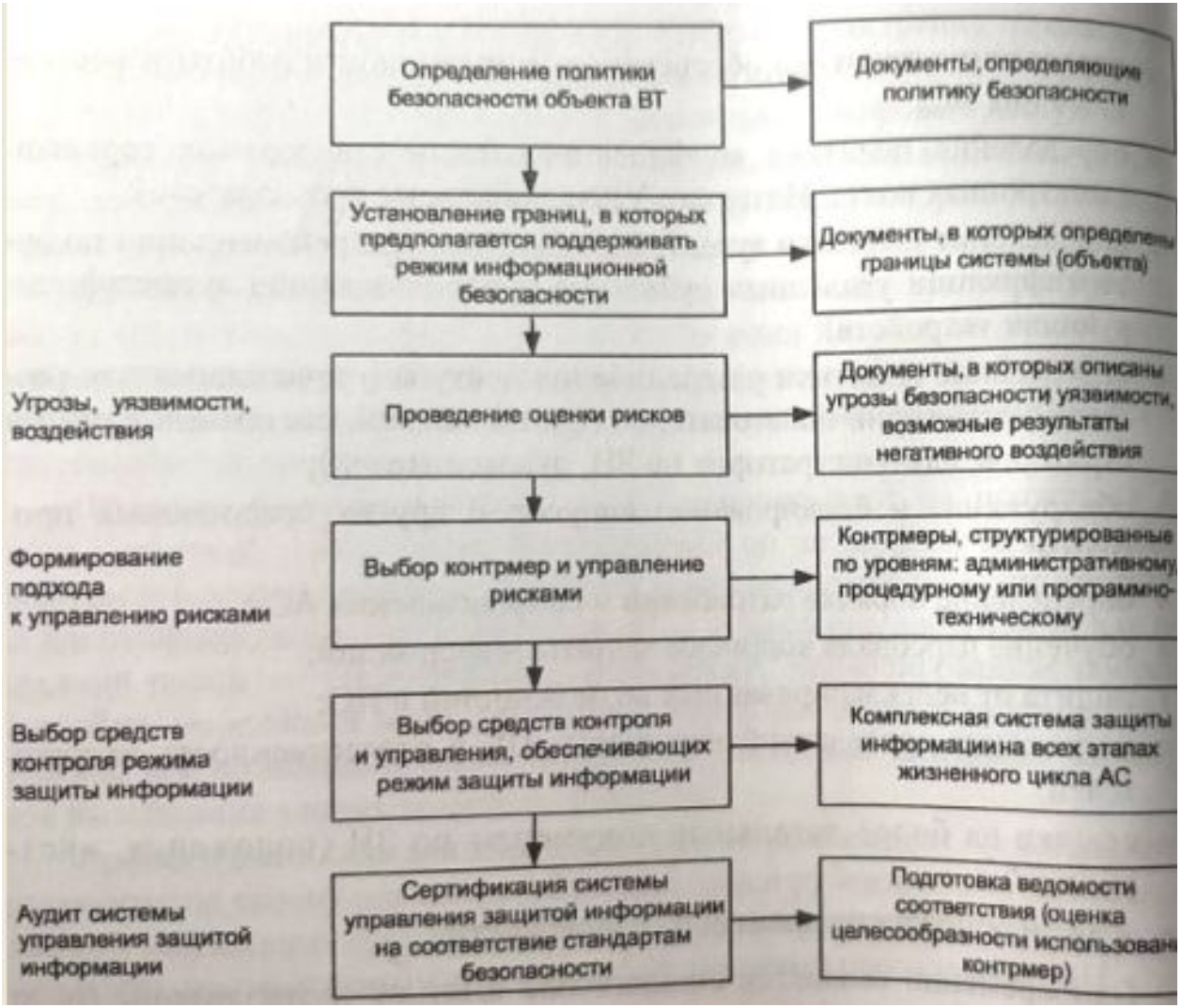
Передача секретной информации

Уничтожение секретной информации

Идентификация и аутентификация

Управление доступом

Основные этапы обеспечения режима защиты информации



Примеры документов («бумажная безопасность»)

МИРЭА
Российский технологический университет

«Концепция обеспечения безопасности в автоматизированной системе организации»
«Защита от несанкционированного доступа к информации незаконного вмешательства в процесс функционирования АС»
«Положение об определении требований по защите категорирования ресурсов в АС»
«Перечень информационных ресурсов подлежащих защите»
«Положение об отделе технической защиты информации»
«Памятка обязанности пользователя»
« Обязанности администратора по защите информации объекта информатизации»
«Инструкция по установке модификации и техническому обслуживанию программного обеспечения и аппаратных средств АС»
«План обеспечения непрерывной работы и восстановления объекта информатизации»
«Инструкция по организации парольной защиты»
«Инструкция по организации антивирусной защиты»
«Инструкция по работе с носителями ключевой информации»

Примеры документов («бумажная безопасность»)

Оценка требований к защищённости информационных ресурсов АС

Субъекты	Уровень ущерба по свойствам информации		
	конфиденциальность	целостность	доступность
№ 1	Нет	Средняя	Средняя
№ 2	Высокая	Средняя	Средняя
№ 3	Низкая	Низкая	Низкая
В итоге	Высокая	Средняя	Средняя

Примеры документов («бумажная безопасность»)

Заявка на должностных лиц, допущенных
к защищаемым ресурсам объекта информатизации

№ п/п	Фамилия и инициалы должностного лица, допущенного к защищаемым ресурсам объекта информатизации	Защищаемые ресурсы			
		полное наименование ресурса	условное наименование ресурса	разрешён доступа	
				чтение	з п
1	2	3	4	5	
1	Стефанович А. Б.	Файл 777.doc	FC375	да	
		Файл verba.exe	EC025	–	
		Файл verba.txt	FC376	да	

Внутренние организационно-распорядительные документы (далее – ОРД) по защите информации.

МИРЭА Российский технологический университет

Что нужно сделать	Требование ФСТЭК	Как реализовать (как выполнено)	Примечание	Статус
Документы и политики, которые нужно разработать в соответствии с документом "Меры по защите информации в государственных информационных системах"				
Правила идентификации и аутентификации пользователей	ИАФ.1	Раздел 3 Политики. П 5.2 инструкции администратора.	Не забыть вписать обязательную двухфакторную аутентификацию для всех удаленных пользователей и администраторов для К2 и обязательную (в том числе и локальную) двухфакторную аутентификацию для всех при К1	Выполнено
Перечень типов устройтсв, подлежащих идентификации и аутентификации + правила и процедуры	ИАФ.2 (К2+)	Необходимость учета и идентификации и аутентификации ТС прописана в инструкции администратора (п. 5.6). В политике п 3.13 и приложение 4.	Так как это нужно для К2+, будет делаться по мере необходимости	Выполнено
Правила и процедуры управления идентификаторами	ИАФ.3	П. 5.8 инструкции администратора		Выполнено
Определить ответственного за хранение, выдачу, инициализации средств аутентификации	ИАФ.4	п. 5.10 инструкции администратора		Выполнено
Правила управления учетными записями пользователей	УПД.1	П. 5.8 инструкции администратора		Выполнено
Правила разграничения доступа	УПД.2	Описание ролей и разграничение в ИСПДн - в политику ИБ (приложение 2 и 3). Разграничение доступа к бумажным носителям - в положение об обработке ПДн, туда же форму акта уничтожения и правила обработки без автоматизации.	Осталось по неавтоматизированной добавить списки в положение об обработке и защите ПДн. Остальное готово.	Выполнено
Правила и процедуры управления информационными потоками (фильтрация, маршрутизация потоков, изменение правил), список разрешенных внешних ресурсов.	УПД.3 (К2+)	П. 6.6 и 6.12 в инструкции администратора - общая необходимость этого процесса. Раздел 4 политики и приложение 6.	Делаться будет исходя из дефолтной политики фильтрации трафика - блокировать все, кроме явно разрешенного.	Выполнено

https://habr.com/ru/company/ic-dv/blog/456508/

Угрозы безопасности ИС

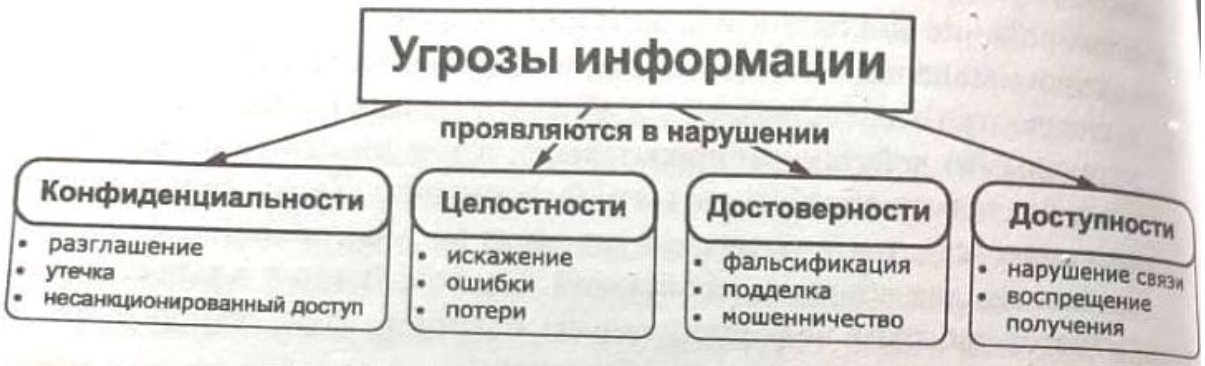


Рис. 1.16. Классификация воздействий угроз на безопасность информации

Рис. 1.17. *Классификация угроз неизменности (целостности) информации*

Угрозы безопасности ИС

Угрозы безопасности ИС

Свойства информации, подверженные влиянию угроз

Способы нанесения ущерба	Объекты воздействий			
	оборудование	программы	данные	персонал
Раскрытие (утечка) информации	Хищение носителей информации, подключение к линии связи, несанкционированное использование ресурсов	Несанкционированное копирование, перехват	Хищение, копирование, перехват	Передача сведений о защите, разглашение, халатность
Потеря целостности информации	Подключение, модификация, специальные вложения, изменение режимов работы, несанкционированное использование ресурсов	Внедрение «троянских коней» и «жучков»	Искажение, модификация	Вербовка персонала, «маскарад»
Нарушение работоспособности автоматизированной системы	Изменение режимов функционирования, вывод из строя, хищение, разрушение	Искажение, удаление, подмена	Искажение, удаление, навязывание ложных данных	Уход, физическое устранение
Незаконное тиражирование (воспроизведение) информации	Изготовление аналогов без лицензий	Использование незаконных копий	Публикация без ведома авторов	

Структура системы защиты информации

Структура системы защиты информации

УБИ = [возможности нарушителя; уязвимости информационной системы;
способ реализации угрозы; последствия реализации от угрозы]

Для каждой эксплуатируемой ИС на основе угроз безопасности в том числе, связанных с действиями нарушителя, разрабатывается модель угроз безопасности информации.

https://bdu.fstec.ru/threat - одна из базы данных. В настоящее время известно
около 60 таких баз

От угрозы риск отличает наличие количественной оценки возможных потерь
и (возможно) оценки вероятности наступления нежелательного события.

Два подхода к обоснованию проекта подсистемы обеспечения безопасности

На практике наибольшее распространение получили два подхода к обоснованию
проекта подсистемы обеспечения безопасности.

Первый из них основан на проверке соответствия уровня защищенности ИС требованиям одного из стандартов в области информационной безопасности.

Тогда критерий достижения цели в области безопасности — это выполнение
заданного набора требований. Критерий эффективности — минимальные суммарные затраты
на выполнение поставленных функциональных требований

Второй

Второй подход к построению системы обеспечения ИБ связан с оценкой и управлением рисками. Изначально он произошел из принципа «разумной достаточности», примененного к сфере обеспечения ИБ.

Два подхода к обоснованию проекта подсистемы обеспечения безопасности

- абсолютно непреодолимую систему защиты создать невозможо;
- необходимо соблюдать баланс между затратами на защиту и получаемым эффектом, в т. ч. и экономическим, заключающимся в снижении потерь от нарушений безопасности;
- стоимость средств защиты не должна превышать стоимости защищаемой информации (или других ресурсов — аппаратных, программных);
- затраты нарушителя на несанкционированный доступ к информации должны превышать то уп.

Идеализированный график соотношения «затраты на защиту — ожидаемые потери»

Риски

МИРЭА
Российский технологический университет

Ресурсом или активом будем называть именованный элемент ИС, имеющий (материальную) ценность и подлежащий защите.

Риск может быть идентифицирован следующим набором параметров:
- угроза, с возможной реализацией которой связан данный риск;
- ресурс, в отношении которого может быть реализована угроза (ресурс может быть информационный, аппаратный, программ-ный и т. д.);
- уязвимость, через которую может быть реализована данная угроза в отношении данного ресурса.

Важно также определить то, как мы узнаем, что нежелательное событие произошло. Поэтому в процессе описания рисков, обычно также указывают события-«*триггеры*», являющиеся идентификато-рами рисков, произошедших или ожидающихся в скором времени (например, увеличение время отклика web-сервера может свидетель-ствовать о производимой на него одной из разновидностей атак на «отказ в обслуживании»).

Риски

МИРЭА Российский технологический университет

Исходя из сказанного выше, в процессе оценки риска надо оценить стоимость ущерба и частоту возникновения нежелательных событий и вероятность того, что подобное событие нанесет урон ресурсу. Размер ущерба от реализации угрозы в отношении ресурса зависит
от стоимости ресурса, который подвергается риску, и степени разрушительности воздействия на ресурс, выражаемой в виде коэффициента разрушительности. Как правило, указанный коэффициент лежит в диапазоне от 0 до 1. Таким образом, получаем оценку потери от разовой реализации угрозы, представимую в виде произведения: $Потери = (Стоим.\ Рес.) \times (Коэфф.\ Разруш.)$.

Далее необходимо оценить частоту возникновения рассматриваемого нежелательного события (за какой-то фиксированный период времени, например, за год) и вероятность успешной реализации угрозы. В результате, стоимость риска может быть вычислена по формуле:

$$Стоим.Риска = (Частота) \times (Вероятн.) \times (Стоим.\ Рес.) \times \times (Коэфф.\ Разруш).$$

Риски

МИРЭА Российский технологический университет

Ожидаемый ущерб сравнивается с затратами на меры и средства защиты, после чего принимается решение в отношении данного риска. Он может быть:

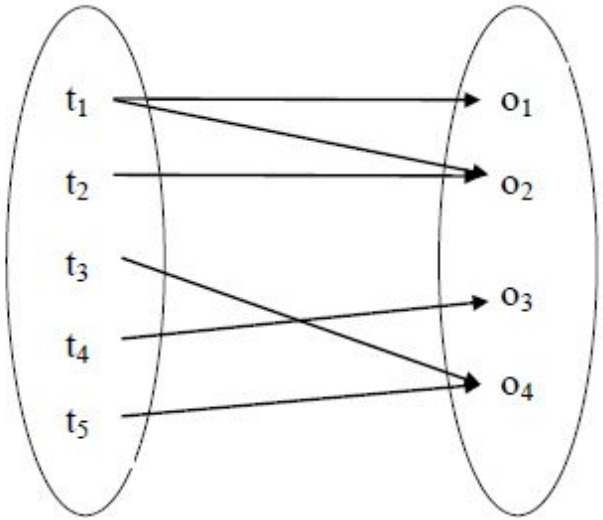
- *принят*;
- *снижен* (например, за счет внедрения средств и механизмов защиты, уменьшающих вероятность реализации угрозы или коэффициент разрушительности);
- *устранен* (за счет отказа от использования подверженного угрозе ресурса);
- *перенесен* (например, застрахован, в результате чего в случае реализации угрозы безопасности потери будет нести страховая компания, а не владелец ИС).

Модель системы безопасности с полным перекрытием строится исходя из постулата, что система безопасности должна иметь, по крайней мере, одно средство для обеспечения безопасности на каждом возможном пути воздействия нарушителя на ИС. В модели точно определяется каждая область, требующая защиты, оцениваются средства обеспечения безопасности с точки зрения их эффективности и их вклад в обеспечение безопасности во всей вычислительной системе.

Двудольный граф «угроза–объект»

Считается, что несанкционированный доступ к каждому из множества защищаемых объектов (ресурсов ИС) **O** сопряжен с некоторой «величиной ущерба» для владельца ИС, и этот ущерб может быть определен количественно.

С каждым объектом, требующим защиты, связывается некоторое множество действий, к которым может прибегнуть нарушитель для получения несанкционированного доступа к объекту. Потенциальные злоумышленные действия по отношению ко всем объектам $o \in \mathbf{O}$ формируют множество угроз ИБ **T**. Каждый элемент данного множества характеризуется вероятностью появления.



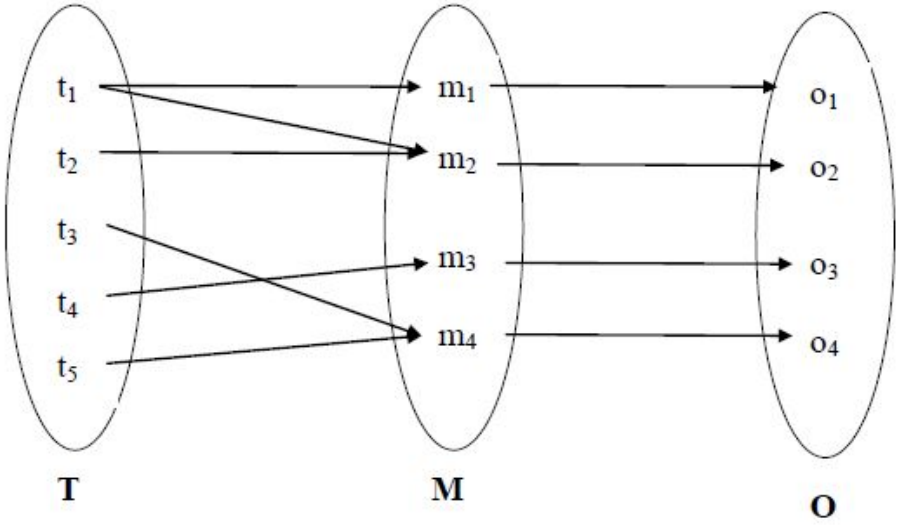
Двудольный граф «угроза–объект»

Множество отношений «угроза–объект» образует двухдольный граф в котором ребро (t_i, o_j) существует тогда и только тогда, когда угроза t_i является средством получения доступа к объекту o_j.

Цель защиты состоит в том, чтобы «перекрыть» каждое ребро данного графа и воздвигнуть барьер для доступа по этому пути.

Трёхдольный граф «угроза–средство безопасности-объект»

Завершает модель третий набор, описывающий средства обеспечения безопасности **M**, которые используются для защиты информации в ИС. В идеальном случае каждое средство $m_k \in \mathbf{M}$ должно устранять некоторое ребро (t_i, o_j). В действительности m_k выполняет функцию «барьера», обеспечивая некоторую степень сопротивления попыткам проникновения. Это сопротивление — основная характеристика, присущая всем элементам набора **M**. Набор **M** средств обеспечения безопасности преобразует двудольный граф в трехдольный



Система Клементса

В защищенной системе все ребра представляются в форме (t_i,m_k) и (m_k,o_j). Любое ребро в форме (t_i,o_j) определяет незащищенный объект. Следует отметить, что одно и то же средство обеспечения безопасности может противостоять реализации более чем одной угрозы и (или) защищать более одного объекта. Отсутствие ребра (t_i,o_j) не гарантирует полного обеспечения безопасности (хотя наличие такого ребра дает потенциальную возможность несанкционированного доступа за исключением случая, когда вероятность появления t_i равна нулю).

Далее в рассмотрение включается теоретико-множественная модель защищенной системы — система обеспечения безопасности Клементса. Она описывает систему в виде пятикортежного набора **S = {O,T,M,V,B}**, где **O** — набор защищаемых объектов; **T** — набор угроз; **M** — набор средств обеспечения безопасности; **V** — набор уязвимых мест — отображение **TxO** на набор упорядоченных пар $V_i = (t_i,o_j)$, представляющих собой пути проникновения в систему; **B** — набор барьеров — отображение **VxM** или **TxOxM** на набор упорядоченных троек $b_i = (t_i,o_j,m_k)$, представляющих собой точки, в которых требуется осуществлять защиту в системе.

Система Клементса

Таким образом, система с полным перекрытием — это система, в которой имеются средства защиты на каждый возможный путь проникновения. Если в такой системе $\exists (t_i,o_j) \in V$, то $\exists (t_i,o_j,m_k) \in B$.

Далее производятся попытки количественно определить степень безопасности системы, сопоставляя каждой дуге весовой коэффициент.

Модель системы безопасности с полным перекрытием описывает требования к составу подсистемы защиты ИС. Но в ней не рассматривается вопрос стоимости внедряемых средств защиты и соотношения затрат на защиту и получаемого эффекта. Кроме того, определить полное множество «путей проникновения» в систему на практике может оказаться достаточно сложно. А именно от того, как полно описано это множество, зависит то, насколько полученный результат будет адекватен реальному положению дел.

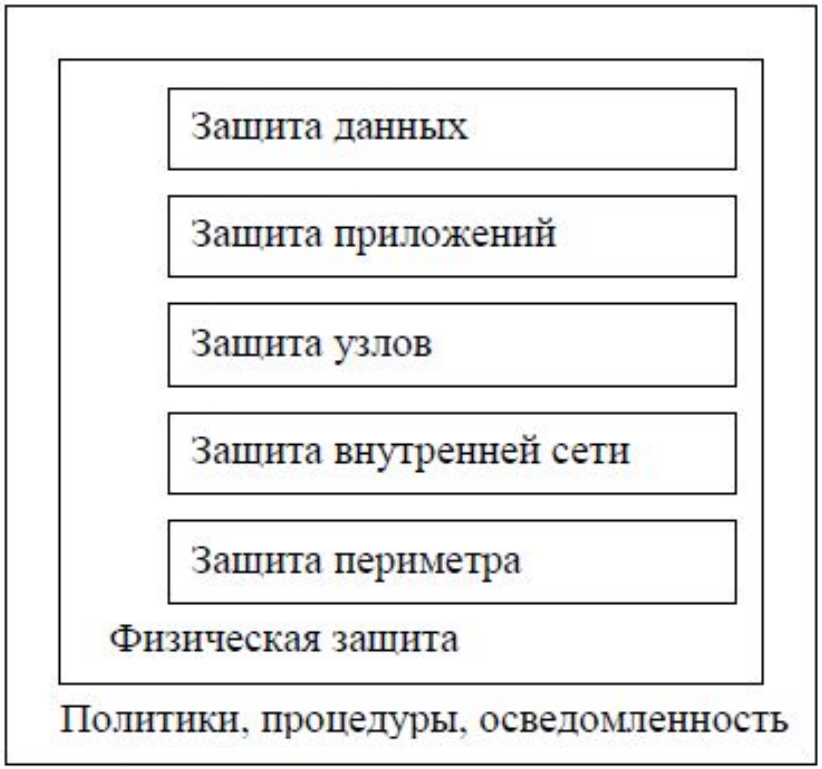
Lifecycle Security

МИРЭА Российский технологический университет

Lifecycle Security — это обобщенная схема построения комплексной защиты компьютерной сети предприятия. Выполнение описываемого в ней набора процедур позволяет системно решать задачи, связанные с защитой информации, и дает возможность оценить эффект от затраченных средств и ресурсов. С этой точки зрения, идеология Lifecycle Security может быть противопоставлена тактике «точечных решений», заключающейся в том, что все усилия сосредотачиваются на внедрении отдельных частных решений

Lifecycle Security

Модель многоуровневой защиты (эшелонированная оборона)



Уровень физической защиты
Уровень защиты периметра
Уровень защиты внутренней сети
Уровень защиты узлов
Уровень защиты приложений
Уровень защиты данных

Методика управления рисками, предлагаемая Майкрософт

- Разработка оценочного листа анализа рисков безопасности
- Измерение эффективности элемента контроля

- Планирование сбора данных о рисках
- Сбор данных о рисках
- Определение приоритетов рисков

- Поиск целостного подхода
- Упорядочивание решений для контроля

- Определение функциональных требований
- Выявление решений по контролю
- Проверка соответствия решений требованиям
- Оценка снижения риска
- Оценка стоимости решения
- Выбор стратегии нейтрализации риска

МЕТОДИКИ И ПРОГРАММНЫЕ ПРОДУКТЫ ДЛЯ ОЦЕНКИ РИСКОВ

- методики, использующие оценку риска на качественном уровне (например, по шкале «высокий», «средний», «низкий»). К таким методикам, в частности, относится FRAP;
- количественные методики (риск оценивается через числовое значение, например размер ожидаемых годовых потерь). К этому классу относится методика RiskWatch;
- методики, использующие смешанные оценки (такой подход используется в CRAMM, методике Майкрософт и т. д.).

Методика CRAMM

- методики, использующие оценку риска на качественном уровне (например, по шкале «высокий», «средний», «низкий»). К таким методикам, в частности, относится FRAP;
- количественные методики (риск оценивается через числовое значение, например размер ожидаемых годовых потерь). К этому классу относится методика RiskWatch;
- методики, использующие смешанные оценки (такой подход используется в CRAMM, методике Майкрософт и т. д.).

Версии программного обеспечения CRAMM, ориентированные на разные типы организаций, отличаются друг от друга своими базами знаний (профилями).

Коммерческий профиль (Commercial Profile), для правительственных организаций — Правительственный профиль (Government profile).

Методика CRAMM

Исследование ИБ системы с помощью CRAMM проводится в три стадии:
На *первой стадии* анализируется все, что касается идентификации и определения ценности ресурсов системы. Ценность физических ресурсов в CRAMM определяется стоимостью их восстановления в случае разрушения.
Ценность данных и программного обеспечения определяется в следующих ситуациях:
- недоступность ресурса в течение определенного периода времени;
- разрушение ресурса — потеря информации, полученной со времени последнего резервного копирования, или ее полное разрушение;
- нарушение конфиденциальности в случаях несанкционированного доступа штатных сотрудников или посторонних лиц;
- модификация — рассматривается для случаев мелких ошибок персонала (ошибки ввода), программных ошибок, преднамеренных ошибок;
- ошибки, связанные с передачей информации: отказ от доставки, недоставка информации, доставка по неверному адресу.

Методика CRAMM

МИРЭА Российский технологический университет

Для оценки возможного ущерба CRAMM рекомендует использовать следующие параметры:

- ущерб репутации организации;
- нарушение действующего законодательства;
- ущерб для здоровья персонала;
- ущерб, связанный с разглашением персональных данных отдельных лиц;
- финансовые потери от разглашения информации;
- финансовые потери, связанные с восстановлением ресурсов;
- потери, связанные с невозможностью выполнения обязательств;
- дезорганизация деятельности.

Методика CRAMM

Для данных и программного обеспечения выбираются применимые к данной ИС критерии, дается оценка ущерба по шкале со значениями от 1 до 10.

В описаниях CRAMM в качестве примера приводится в [21] такая шкала оценки по критерию «Финансовые потери, связанные с восстановлением ресурсов»:

- 2 балла — менее $ 1000;
- 6 баллов — от $ 1000 до $ 10 000;
- 8 баллов — от $ 10 000 до $ 100 000;
- 10 баллов — свыше $ 100 000.

При низкой оценке по всем используемым критериям (3 балла и ниже) считается, что рассматриваемая система требует базового уровня защиты (для этого уровня не требуется подробной оценки угроз ИБ) и вторая стадия исследования пропускается.

Методика CRAMM

На *второй стадии* анализа рассматривается все, что относится к идентификации и оценке уровней угроз для групп ресурсов и их уязвимостей. В конце стадии заказчик получает идентифицированные и оцененные уровни рисков для своей системы.
Программное обеспечение CRAMM для каждой группы ресурсов и каждого из 36 типов угроз генерирует список вопросов, допускающих однозначный ответ. Уровень угроз оценивается, в зависимости от ответов, как очень высокий, высокий, средний, низкий и очень низкий. Уровень уязвимости оценивается, в зависимости от ответов, как высокий, средний и низкий.
На основе этой информации рассчитываются уровни рисков в дискретной шкале с градациями от 1 до 7. Полученные уровни угроз, уязвимостей и рисков анализируются и согласовываются с заказчиком.

Методика CRAMM

Основной подход для решения этой проблемы состоит в рассмотрении [2]:

- уровня угрозы
- уровня уязвимости
- размера ожидаемых финансовых потерь

Шкала оценки уровней угрозы (частота возникновения)

Описание	Значение
инцидент происходит в среднем не чаще, чем каждые 10 лет	очень низкий (very low)
инцидент происходит в среднем один раз в 3 года	низкий (low)
инцидент происходит в среднем раз в год	средний (medium)
инцидент происходит в среднем один раз в четыре месяца	высокий (high)
инцидент происходит в среднем раз в месяц	очень высокий (very high)

Методика CRAMM

МИРЭА Российский технологический университет

Матрица ожидаемых годовых потерь

		0,1	0,1	0,1	0,34	0,34	0,34	1	1	1	3,33	3,33	3,33	10	10	10
		0,1	0,5	1	0,1	0,5	1	0,1	0,5	1	0,1	0,5	1	0,1	0,5	1
1	1000	10	50	…												10^4
2	10000	100	…													…
3	30000	3×10^2														
4	10^5	10^3														
5	3×10^5	3×10^3														
6	10^6	10^4														
7	3×10^6	3×10^4														
8	10^7	10^5														
9	3×10^7	3×10^5														
10	10^8	10^6														10^9

Исходя из оценок стоимости ресурсов защищаемой ИС, оценок угроз и уязвимостей, определяются «ожидаемые годовые потери». В
таблице приведен пример матрицы оценки ожидаемый потерь. В ней второй столбец слева содержит значения стоимости ресурса, верхняя строка заголовка таблицы — оценку частоты возникновения
угрозы в течение года (уровня угрозы), нижняя строка заголовка —
оценку вероятности успеха реализации угрозы (уровня уязвимости).

Литература

МИРЭА
Российский технологический университет

1. М.А. Борисов, И.В.Заводцев, И.В. Чижов Основы программно-аппаратной защиты информации
2. С.А. Нестеров Основы информационной безопасности

Спасибо за внимание!