Система управления информационной безопасностью. Угрозы информационной безопасности

Толстой Александр Иванович

НИЯУ МИФИ,

факультет «Кибернетика и информационная безопасность»,

кафедра «Информационная безопасность банковских систем»

Москва, 2016

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Безопасность информации:

- *состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз*

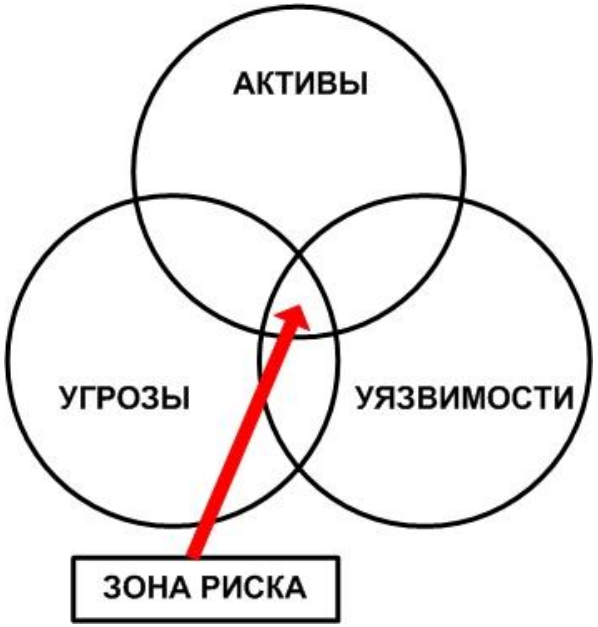
Руководящий документ Гостехкомиссии России от 30 марта 1992 г. «Защита от несанкционированного доступа к информации. Термины и определения»

- *состояние защищенности информации, при котором обеспечивается ее конфиденциальность, доступность и целостность*

Рекомендациям по стандартизации Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации» и ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

- *Угроза потенциальная причина инцидента, который может нанести ущерб системе или организации* **[ГОСТ Р ИСО/МЭК 13335-1-2006];**
- *Угроза ИБ - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации* **[ГОСТ Р 50922-2006];**

«Угроза ИБ» - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации **[ГОСТ Р 50922-2006];**



«Актив» - все, что имеет ценность для организации **[ГОСТ Р ИСО/МЭК 13335-1-2006];**

«Уязвимость» (брешь) (vulnerability) - слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами **[ГОСТ Р ИСО/МЭК 13335-1-2006];**

Если уязвимость соответствует угрозе, то существует

Принципы управления ИБ:

Принципы обеспечения ИБ организации

Опыт

От чего защищаем?

Модель угроз ИБ

Модель нарушителя ИБ

Идентификация активов и биз-нес-процессов

Мониторинг

Как контролируем?

Оценка рисков ИБ

Политика ИБ организации

Аудит

Что защищаем?

Реализация политики ИБ организации

Как защищаем?

ГОСТ Р ХХХХХ-201Х Защита информации ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ОБЪЕКТЫ ИНФОРМАТИЗАЦИИ. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. Общие положения (проект, первая редакция)

- ***Угроза ИБ*** *- совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации* **[ГОСТ Р 50922-2006];**

- ***Причинами возникновения угроз безопасности информации являются:***

- преднамеренные действия нарушителей (злоумышленников);
- непреднамеренные действия (ошибки персонала);
- отказы и сбои в работе оборудования (неполадки в работе технических и программных средств, в т.ч. и вследствие форс-мажорных обстоятельств);
- наличие уязвимостей объекта информатизации.

Опеределение:

•Объект информатизации: *Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения переговоров*

Объект информатизации = актив

В качестве основных видов ОИ рассматриваются:

а) автоматизированные рабочие места и информационные системы (ИС)

- автоматизированные рабочие места без подключения к внешним информационным системам, в том числе к сетям общего пользования;

- автоматизированные рабочие места с подключением к внешним информационным системам, в том числе к сетям общего пользования;

- локальные ИС без подключения к внешним ИС, в том числе к сетям общего пользования;

- локальные ИС с подключением к внешним ИС, в том числе к сетям общего пользования;

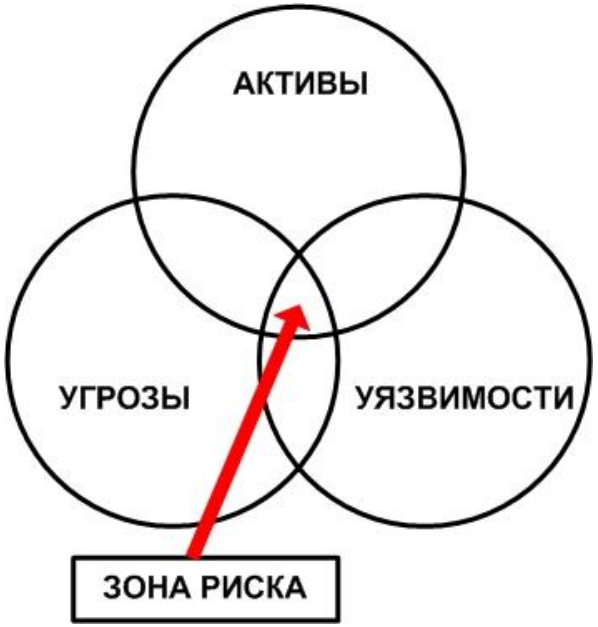
- распределенные ИС без подключения к внешним информационным системам и сетям общего пользования;

- распределенные ИСс подключением к внешним информационным системам и сетям общего пользования;

б) средства изготовления и размножения документов, использующие методы обработки информации, не предусматривающие использование ЭВМ;

в) средства обработки речевой и видовой информации, эксплуатация которых не предусматривает использование ЭВМ;

«Угроза ИБ» - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации **[ГОСТ Р 50922-2006];**



«Актив» - все, что имеет ценность для организации **[ГОСТ Р ИСО/МЭК 13335-1-2006];**

«Уязвимость» (брешь) (vulnerability) - слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами **[ГОСТ Р ИСО/МЭК 13335-1-2006];**

Если уязвимость соответствует угрозе, то существует

Выявление и оценка опасности угроз безопасности информации на ОИ осуществляется путем определения уязвимостей ОИ и возможности реализации всего множества угроз безопасности информации (в технических, программных и программно-технических средствах обработки информации, средствах обеспечения функционирования ОИ и т.п.) на всех этапах обработки защищаемой информации.

Угрозы безопасности информации реализуются в результате:

- ***НСД к информации в ИС (воздействий на информацию и ее носители);***
- ***утечки информации по техническим каналам.***

Основными признаками классификации угроз НСД к информации в ИС (воздействий на информацию) являются:

- ***вид источника угрозы безопасности информации (нарушитель безопасности информации);***
- ***классы уязвимостей ИС;***
- ***способы реализации угроз безопасности информации;***
- ***последствия нарушения безопасности информации.***

Основными признаками классификации угроз утечки информации по техническим каналам являются.

- вид источника угрозы безопасности информации;

- среда распространения информативного сигнала;

- вид источника защищаемой информации;

- последствия нарушения безопасности информации.

Угрозы безопасности информации представляются в моделях угроз безопасности информации для конкретных объектов (их видов, составных частей),

Содержание модели (описание):

- **ОИ и его структурно-функциональных характеристик,**
- **возможностей нарушителей (модель нарушителя),**
- **возможных уязвимостей ОИ,**
- **способов реализации угроз безопасности информации**
- **последствий от нарушения свойств**

Формализованное представление описания угроз:

Угроза НСД к информации: = <(источник угрозы (нарушитель)>, <уязвимость ИС>, <способ реализации угрозы>, <последствия реализации угрозы>.

Угроза утечки информации по техническим каналам: = <источник угрозы>, <среда распространения информативного сигнала>, <источник защищаемой информации>, <последствия реализации угрозы>.

Виды моделей угроз:

- базовые модели угроз безопасности информации для видов защищаемой информации;
- базовые модели угроз безопасности информации для различных видов ОИ;
- частные модели угроз безопасности информации для конкретных ОИ.

Разделы модели угроз (общий случай):

- назначение модели;

- нормативные ссылки;

- термины и определения;

- основные положения;

- описание ОИ и его структурно-функциональных характеристик;

- классификация угроз безопасности информации;

- описание угроз безопасности информации (см.формулу).

В разделе «Назначение модели» указывается:

- вид модели угроз безопасности информации (в соответствии классификацией моделей);
- цель (цели) разработки модели;
- состав предполагаемых пользователей модели;
- область применения модели и краткая характеристика решаемых с ее использованием задач.

В разделе «Нормативные ссылки» приводится **перечень стандартов, нормативных правовых актов (при необходимости) и других документов, ссылки на которые приводятся в модели.**

Раздел «Термины и определения» включает:

- термины и определения, используемые в других документах со ссылкой на них;
- новые термины и определения (при необходимости).

В разделе «Основные положения» приводится краткая характеристика:

- объекта (объектов) информатизации и видов защищаемой информации, для которого разрабатывается модель угроз безопасности информации;

- содержания основных разделов модели угроз.

В разделе «Описание ОИ и его структурно-функциональных характеристик» приводится:

- описание структуры и состава ОИ, физических, логических, функциональных и техно-логических взаимосвязей между сегментами (составными частями) ОИ, с иными ОИ и инфор-мационно-телекоммуникационными сетями;

- режимы обработки информации на ОИ и в его отдельных сегментах (составных частях);

- описание иных характеристик ОИ, применяемых

Раздел «Классификация угроз безопасности информации» должен содержать:

- состав (перечень) признаков классификации, используемых в модели угроз;
- принятую схему классификации угроз в разрабатываемой модели.

Схема классификации может быть представлена:

- по определенной форме, с учетом выбранных признаков классификации;
- в графической (например, в виде схемы, отражающей связи между признаками) или табличной форме.

Раздел «Описание угроз безопасности информации» разрабатывается

с учетом характеристик угроз безопасности информации;

с использованием правил описания угроз безопасности информации, представленных в предыдущих разделах.

В разделе приводится:

-- описание возможностей нарушителей (модель нарушителя);

-- формализованное описание угроз.

Последствия нарушения безопасности информации характеризуются **нарушением конфиденциальности, целостности и доступности информации.**

Последствиями нарушения конфиденциальности защищаемой информации являются

- **неконтролируемое распространение защищаемой информации в результате НСД к ней,**
- **получение защищаемой информации заинтересованными в ней субъектами.**

Последствиями нарушения целостности защищаемой информации являются ее уничтожение и/ или модификация.

Последствием нарушения доступности защищаемой информации является исключение возможности использования этой информации ее обладателем (пользователем), процессом или устройством.

Последствия нарушения целостности и доступности информации включают в себя уничтожение (вывод из строя), искажение (модификацию), блокирование:

- системного ПО, обеспечивающего функционирование ИС (операционной системы, драйверов устройств, микропрограмм, коммуникационных протоколов и т.п.);
- прикладных программ общего применения (текстовых, графических редакторов, систем управления базами данных и т.п.);
- прикладного ПО пользователя (программ, разработанных и установленных в интересах выполнения задач пользователем);
- информации, циркулирующей в ИС;
- программного обеспечения средств защиты информации в составе ИС;
- передаваемых по средствам коммуникаций информативных сигналов (путем постановки помех в диапазоне частот передаваемых сигналов, экранирования и т.п.);
- программно-аппаратных и аппаратных элементов в составе ИС путем электромагнитного воздействия на

Угрозы утечки информации по техническим каналам обусловлены наличием возможности регистрации, перехвата, приема, съема информации, воздействия на носитель информации с использованием технических средств.

Источником (носителем) защищаемой информации является материальный объект, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Последствия нарушения безопасности информации характеризуются нарушением ее конфиденциальности в результате получения защищаемой информации заинтересованным

РС БР ИББС-2.2 «Обеспечение ИБ организаций банковской системы Российской Федерации. Методика оценки рисков нарушения ИБ»:

Угроза ИБ: угроза нарушения свойств ИБ — доступности, целостности или конфиденциальности информационных активов организации БС РФ.

Ущерб: утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры организации или другой вред активам и (или) инфраструктуре организации БС РФ, наступивший в результате реализации угроз ИБ через уязвимости ИБ.

Модель угроз ИБ (структура модели угроз ИБ) – это описание: источников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, используемых источниками угроз ИБ; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба.

РС БР ИББС-2.2 «Обеспечение ИБ организаций банковской системы Российской Федерации. Методика оценки рисков нарушения ИБ»:

Угроза ИБ: угроза нарушения свойств ИБ — доступности, целостности или конфиденциальности информационных активов организации БС РФ.

Источник угрозы ИБ: объект или субъект, реализующий угрозы ИБ путем воздействия на объекты среды информационных активов организации БС РФ.

Угрозы ИБ реализуются их источниками (источниками угроз ИБ), которые могут воздействовать на объекты среды информационных активов организации БС РФ. В случае успешной реализации угрозы ИБ информационные активы теряют часть или все свойства ИБ.

Если источником угрозы является субъект, то разрабатывается **модель нарушителя**

РС БР ИББС-2.2 «Обеспечение ИБ организаций банковской системы Российской Федерации. Методика оценки рисков нарушения ИБ»:

Для оценки рисков необходимо дополнить модель угроз следующими оценками :

— степень возможности реализации угроз ИБ (СВР угроз ИБ), выявленными и (или) предполагаемыми источниками угроз ИБ в результате их воздействия на объекты среды рассматриваемых типов информационных активов;

— степени тяжести последствий от потери свойств ИБ для рассматриваемых типов информационных активов (СТП нарушения ИБ).

Оценка СВР угроз ИБ и СТП нарушения ИБ базируется на экспертной оценке, выполняемой сотрудниками службы ИБ организации БС РФ с привлечением сотрудников подразделений информатизации.

РС БР ИББС-2.2 «Обеспечение ИБ организаций банковской системы Российской Федерации. Методика оценки рисков нарушения ИБ»:

Шкала оценки степени возможности реализации (СВР) угрозы ИБ:

- нереализуемая;
- минимальная;
- средняя;
- высокая;
- критическая

Шкала оценки степени тяжести последствий (СТП) угрозы ИБ:

- минимальная;
- средняя;
- высокая;
- критическая.

РС БР ИББС-2.2 «Обеспечение ИБ организаций банковской системы Российской Федерации. Методика оценки рисков нарушения ИБ»:

Основными факторами для оценки степени возможности реализации (СВР) угроз ИБ являются:

- данные о расположении источника угрозы относительно соответствующих типов объектов среды;
- информация о мотивации источника угрозы (для источников угроз антропогенного характера);
- предположения о квалификации и (или) ресурсах источника угрозы;
- статистические данные о частоте реализации угрозы ее источником в прошлом;
- информация о способах реализации угроз ИБ;
- информация о сложности обнаружения реализации угрозы рассматриваемым источником;
- данные о наличии у рассматриваемых типов объектов среды организационных, технических и прочих априорных защитных мер.

РС БР ИББС-2.2 «Обеспечение ИБ организаций банковской системы Российской Федерации. Методика оценки рисков нарушения ИБ»:

Основными факторами для оценки степени тяжести последствий (СТП) нарушения ИБ являются:

- **степень влияния на непрерывность деятельности организации;**
- **степень влияния на деловую репутацию;**
- **объем финансовых и материальных потерь;**
- **объем финансовых и материальных затрат, необходимых для восстановления свойств ИБ для информационных активов (ИА) рассматриваемого типа и ликвидации последствий нарушения ИБ;**
- **объем людских ресурсов, необходимых для восстановления свойств ИБ для ИА рассматриваемого типа и ликвидации последствий нарушения ИБ;**
- **объем временных затрат, необходимых для восстановления свойств ИБ для ИА рассматриваемого типа и ликвидации последствий нарушения ИБ;**

РС БР ИББС-2.2 «Обеспечение ИБ организаций банковской системы Российской Федерации. Методика оценки рисков нарушения ИБ»:

Основными факторами для оценки степени тяжести последствий (СТП) нарушения ИБ являются:

- **степень нарушения законодательных требований и (или) договорных обязательств организации;**
- **степень нарушения требований регулирующих и контролирующих (надзорных) органов в области ИБ, а также требований нормативных актов Банка России;**
- **объем хранимой, передаваемой, обрабатываемой, уничтожаемой информации, соответствующей рассматриваемому типу объекта среды;**
- **данные о наличии у рассматриваемых типов объектов среды организационных, технических и прочих апостериорных защитных мер.**

РС БР ИББС-2.2 «Обеспечение ИБ организаций банковской системы Российской Федерации. Методика оценки рисков нарушения ИБ»:

Модель угроз (описание):

- источников угроз ИБ;
- методов реализации угроз ИБ;
- объектов, пригодных для реализации угроз ИБ;
- уязвимостей, используемых источниками угроз ИБ;
- типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов);
- масштабов потенциального ущерба;
- степень возможности реализации угроз ИБ (СВР угроз ИБ), выявленными и (или) предполагаемыми источниками угроз ИБ в результате их воздействия на объекты среды рассматриваемых типов информационных активов;
- степени тяжести последствий от потери свойств ИБ для рассматриваемых типов информационных активов .

РС БР ИББС-2.2 «Обеспечение ИБ организаций банковской системы Российской Федерации. Методика оценки рисков нарушения ИБ»:

Модель нарушителя:

- данные о расположении нарушителя относительно соответствующих типов объектов среды;
- информация о мотивации нарушителя;
- предположения о квалификации и (или) ресурсах нарушителя;
- статистические данные о частоте реализации угрозы нарушителем в прошлом;
- информация о способах реализации угроз ИБ нарушителем;
- Описание объектов, пригодных для реализации угроз ИБ;
- Описание уязвимостей, используемых источниками угроз ИБ;
- Описание типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности ИА);
- Описание масштабов потенциального ущерба;
- Оценка степени возможности реализации угроз ИБ (СВР угроз ИБ), выявленными и (или) предполагаемыми нарушителями в результате их воздействия на объекты среды рассматриваемых типов ИА;
- Оценка степени тяжести последствий от потери свойств ИБ для рассматриваемых типов ИА

Благодарю за внимание!

Толстой Александр Иванович

AITolstoj@mephi.ru

8(499)324-97-35