Курс лекций

Средства и методы защиты информации

Коротких Вячеслав Владимирович
канд. экон. наук, доц. кафедры информационных технологий и математических методов в экономике
ФГБОУ ВО «ВГУ»

Организационные меры защиты информации

Лекция 3

Содержание лекции

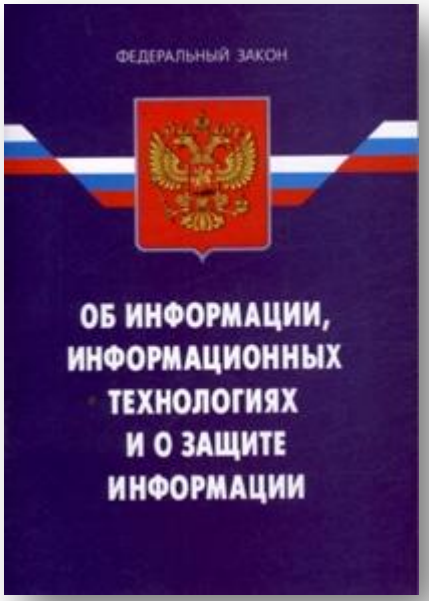
- Законодательные меры ЗИ
- Административные меры ЗИ
  - Управление рисками
  - Политика безопасности организации
  - Управление персоналом
  - Планирование действий в ЧС
- Организационно-технические меры ЗИ
  - Физическая защита ОИ
  - Защита поддерживающей инфраструктуры

Законодательные меры ЗИ

- Снижение вероятности техногенных угроз
- Снижение ущерба от стихийных явлений
- Снижение вероятности угроз, реализуемых по причине халатности или недостаточной квалификации
- Защита от нарушителей, действующих из любопытства или самоутверждения
- Защита от нарушителей, действующих преднамеренно и целенаправленно

Законодательные меры ЗИ

Об информации, информационных технологиях и о защите информации : федер. закон от 27.07.2006 N **149-ФЗ** (ред. от 30.12.2020)



Законодательные меры ЗИ

Статья 16*: Защита информации

Защита информации представляет собой принятие правовых, организационных, технических мер

* **Об информации, информационных технологиях и о защите информации :** федер. закон от 27.07.2006 N **149-ФЗ** (ред. от 30.12.2020)

Законодательные меры ЗИ

Статья 16*: Защита информации

Перечисленные меры направлены на:

1) обеспечение **защиты** информации от неправомерных действий в отношении такой информации
2) соблюдение **конфиденциальности** информации ограниченного доступа
3) реализацию **права на доступ** к информации

Законодательные меры ЗИ

Статья 16*: Защита информации

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства РФ об информации, информационных технологиях и о защите информации

Законодательные меры ЗИ

Статья 16*: Защита информации

4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством РФ, обязаны обеспечить: [выдержки из перечня]

- **предотвращение** несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное **обнаружение** фактов несанкционированного доступа к информации;

Законодательные меры ЗИ

- **недопущение** воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность незамедлительного **восстановления** информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный **контроль** за обеспечением уровня защищенности информации;

Законодательные меры ЗИ

Статья 16*: Защита информации

5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются (уполномоченными федеральными органами исполнительной власти). При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

Такие требования содержатся в соответствующем приказе ФСТЭК России

Законодательные меры ЗИ

Статья 17*

1. Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Законодательные меры ЗИ

Уголовно наказуемые деяния, связанные с нарушением информационной безопасности:

- Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений
- Незаконный оборот специальных технических средств, предназначенных для негласного получения информации
- Нарушение авторских и смежных прав
- Нарушение изобретательских и латентных прав
- Мошенничество в сфере компьютерной информации
- Неправомерный оборот средств платежей

Законодательные меры ЗИ

Уголовно наказуемые деяния, связанные с нарушением информационной безопасности:

- Разглашение государственной тайны
- Неправомерный доступ к компьютерной информации
- Создание, использование и распространение вредоносных компьютерных программ
- Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
- Различные деяния, включающие нарушение безопасности информации как составную часть

Административные меры ЗИ

- Включают правила **доступа** и работы с информацией, установленные руководством организации

- Направлены на персонал организации, а также на его взаимодействие с лицами, находящимися на контролируемой территории в силу их обязанностей или исполняемых организацией функций

Административные меры ЗИ

- Должны соответствовать действующим законам и иным нормативно-правовым актам, не только в сфере защиты информации

- Могут опираться на законодательные меры как
  - На обоснование конкретных административных мер
  - На обоснование запрета конкретных действий
  - Источник санкций за нарушение конкретных мер

Административные меры ЗИ

- Должны поддерживаться организационно-техническими и программно-техническими мерами защиты информации
- Должны соответствовать официальной и фактической позиции руководства организации
- Должны быть доведены до сведения всех сотрудников организации, их исполнение должно контролироваться

Административные меры ЗИ

- Составляют совокупность взглядов руководства на все ситуации, возникающие при хранении, обработке и передаче информации, а также конкретные указания на необходимые действия в таких ситуациях - как штатных, так и экстренных

- Во многом являются определяющими для фактического уровня эффективности системы информационной безопасности организации

Административные меры ЗИ

Включают:

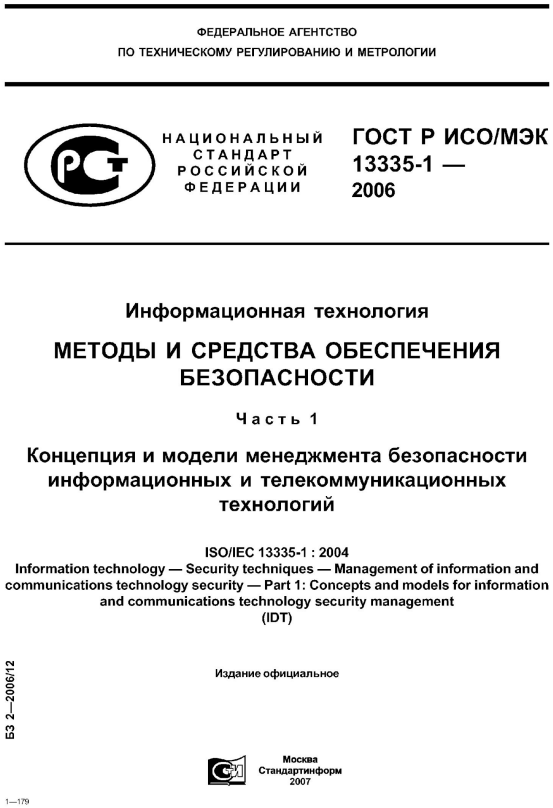
- Управление рисками
- Разработку политики безопасности организации
- Управление персоналом
- Планирование действий в чрезвычайных ситуациях

Управление рисками

«Информационная технология. Методы и средства обеспечения безопасности.

Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»

* ГОСТ Р ИСО/МЭК 27001-2006



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 13335-1 — 2006

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Часть 1

Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

ISO/IEC 13335-1 : 2004
Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management
(IDT)

Издание официальное

БЗ 2—2006/12

Москва
Стандартинформ
2007

1—179

Управление рисками

Активы - все, что имеет ценность для организации

Управление рисками

Риск - потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимости актива или группы активов. Определяется как **сочетание вероятности события** и его **последствий.**

Управление рисками

Менеджмент риска (управление риском) - полный процесс идентификации, контроля, устранения или уменьшения последствий опасных событий, которые могут оказать влияние на ресурсы информационно телекоммуникационных технологий

Управление рисками

- **Оценка риска** - процесс, объединяющий идентификацию риска, анализ риска и оценивание риска
- **Анализ риска** - систематический процесс определения величины риска
- **Обработка риска** - процесс выбора и осуществления мер по модификации риска
- **Остаточный риск** - риск, остающийся после его обработки

Управление рисками

Включает:

- **Оценку** (измерение) рисков - оценку вероятности реализации угрозы и ее возможного ущерба, возможно, выраженного в финансовых потерях

- **Нейтрализацию** рисков - выбор эффективных мер защиты или реагирования на реализацию угрозы

Управление рисками

Защитная мера - сложившаяся практика, процедура или механизм обработки риска

Управление рисками

Этапы управления рисками:

1. Выбор анализируемых объектов и уровня детализации их рассмотрения;
2. Выбор методики оценки рисков;
3. Идентификация активов;
4. Анализ угроз и их последствий, выявление уязвимых мест в защите;
5. Оценка рисков.
6. Выбор защитных мер.
7. Реализация и проверка выбранных мер.
8. Оценка остаточного риска.

Управление рисками

Возможные защитные меры:

- ликвидация риска;
- уменьшение риска;
- принятие риска;
- переадресация риска.

Управление рисками

Рекомендуется включать управление рисками в жизненный цикл ИС и реализовывать защитные меры на различных его этапах:

- Этап **проектирования** ИС - выработка адекватных требований к ИС и ее системе безопасности
- Этап **разработки** ИС - выбор наименее уязвимых решений, минимизация уязвимостей

Политика безопасности организации

Политика безопасности информационно-телекоммуникационных технологий (политика безопасности ИТТ) - правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и ее информационно-телекоммуникационных технологий управлять, защищать и распределять активы, в том числе критичную информацию

Политика безопасности организации

Политика безопасности организации (ПБ) - совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов

Политика безопасности организации

Цели политики безопасности:

- Формирование системы взглядов на проблему обеспечения безопасности информации в организации и пути ее решения с учетом современных технологий обработки и защиты информации;
- Формулирование рекомендаций по повышению степени защищенности ИС;
- Выработка общих требований к мерам защиты информации

Политика безопасности организации

Может рассматриваться как совокупность 3 уровней:

- **Верхний уровень** - решения, касающиеся организации в целом в терминах целостности, доступности, конфиденциальности
- **Средний уровень** - область применения политики безопасности, вопросы ответственности за соблюдение политики безопасности, обучения персонала
- **Нижний уровень** - решения по конкретным системам и сервисам

Политика безопасности организации

Примеры элементов ПБ верхнего уровня:

- Формулировка целей, которые преследует организация в области информационной безопасности;
- Обеспечение базы для соблюдения законов и прочих нормативных актов;
- Формулировка административных решений по вопросам, касающимся организации в целом

Политика безопасности организации

Примеры элементов ПБ среднего уровня:

- Область применения ПБ;
- Обязанности должностных лиц, отвечающих за выполнение ПБ;
- Обучение и информирование персонала о ПБ организации.

Управление персоналом

Включает следующие мероприятия:

- Внедрение должностных инструкций сотрудников:
  - Разделение обязанностей,
  - Минимизация привилегий.
- Информирование и обучение персонала;
- Внедрение инструкций по работе со средствами ЗИ;
- Внедрение инструкций для внештатных ситуаций;
- Разграничение доступа сотрудников:
  - Логического в рамках ИС,
  - Физического в рамках ОИ;
- Контроль, протоколирование и аудит действий персонала.

Управление персоналом

Направлено на решение следующих задач:

- Разделение сферы ответственности сотрудников;
- Противодействие злоумышленным действиям внутренних нарушителей;
- Снижение угроз, реализуемых из-за халатности или недостаточной квалификации сотрудников;
- Снижение последствий угроз, имеющих техногенные или стихийные источники

Планирование действий в ЧС

Направлено на **минимизацию последствий** от таких ситуаций как с физической (выход из строя аппаратного обеспечения, систем и средств обработки информации), так и с финансовой (денежные потери организации) точки зрения

Планирование действий в ЧС

Должно охватывать следующие ситуации:

- Стихийные бедствия
- Аппаратные сбои ИС
- Программные сбои ИС
- Выход из строя поддерживающих коммуникаций
- Обнаружение действий нарушителя

Планирование действий в ЧС

Заключается в:

- Разработке инструкции по действию персонала в перечисленных ситуациях,
- Назначении ответственных лиц за действия в таких ситуациях;
- Информировании сотрудников о необходимых действиях;
- Обучении сотрудников требуемым действиям

Планирование действий в ЧС

Может решать следующие задачи:

- Сохранение функционирования ИС объекта информатизации;
- Снижение убытков организации;
- Обеспечение целостности и доступности информации;
- Прекращение действий нарушителя или усиления последствий угрозы;
- Обеспечение возможности протоколирования и аудита событий;
- Оценка защищенности ОИ от ситуаций подобного рода;
- Принятие мер по снижению риска ситуаций подобного рода.

Планирование действий в ЧС

Примеры действий персонала в ЧС:

- Отключение и эвакуация носителей информации;
- Принятие мер для защиты аппаратного обеспечения ИС от физических повреждений;
- Информирование службы безопасности организации;
- Приостановление работы в штатном режиме;
- Включение систем резервирования;
- Восстановление работоспособности программного обеспечения ИС из резервной копии;
- Замена или ремонт аппаратного обеспечения ИС
- Выявление уязвимостей, приведших к реализации угрозы их устранение

Организационно-технические меры ЗИ

Заключаются в совокупности организационных и технических мероприятий, направленных на:

- контроль доступа на контролируемую территорию и к конкретным объектам ОИ,
- защиту элементов ИС и имущества организации от хищения, повреждения и иных неправомерных действий,
- поддержку работоспособности ИС

Организационно-технические меры ЗИ

Направлены, главным образом, на противодействие:

- Угрозам, имеющим стихийные и техногенные источники;
- Внешним нарушителям, стремящимся получить физический доступ к ИС;
- Внутренним нарушителям, действующим в нарушение своих должностных инструкций

Организационно-технические меры ЗИ

Включают следующие основные мероприятия:

- Контроль доступа на контролируемую территорию и в конкретные помещения;
- Физическая защита ОИ от неправомерных действий;
- Защита поддерживающей инфраструктуры, техническая безопасность.

Физическая защита ОИ

Может включать следующие меры:

- защита от несанкционированного доступа в помещения;
- защита от краж;
- защита от вандализма;
- противопожарная охрана;
- защита от взрывов;
- защита от других неправомерных действий.

Физическая защита ОИ

- Система физической защиты (СФЗ) - совокупность людей, процедур и оборудования, защищающих объект информатизации в целом и его части от действий, нарушающих его безопасность

- СФЗ является основным элементом физической защиты ОИ

Физическая защита ОИ

Целью СФЗ является **предотвращение** реализации квалифицированным нарушителем явных или скрытых неправомерных воздействий на объект информатизации, его ИС, персонал или поддерживающую инфраструктуру

Физическая защита ОИ

Подходы к реализации СФЗ:

- Сдерживание
- Обнаружение - задержка - реагирование

Физическая защита ОИ

Сдерживание заключается в реализации мер, снижающих привлекательность объекта как потенциальной цели воздействия для нарушителя.

Примеры - наличие охраны, видеонаблюдения, сигнализации, ясно видимых потенциальным нарушителем.

Результат сдерживания - отказ нарушителя от попыток реализации угрозы.

Физическая защита ОИ

Обнаружение - выявление скрытой или явной попытки нарушителя проникнуть на контролируемую территорию объекта информатизации.

Показатели эффективности обнаружения:

- Вероятность выявления попытки проникновения;
- Время оценивания попытки;
- Время передачи сообщения о попытке;
- Частота ложных обнаружений.

Физическая защита ОИ

Задержка - замедление продвижения нарушителя к цели.

Способы задержки:

- физические барьеры, препятствия,
- замки,
- персонал охраны.

Показатель эффективности задержки - время на преодоление нарушителем всех препятствий после его обнаружения

Физическая защита ОИ

Реагирование - действия сил СФЗ по воспрепятствованию успеху нарушителя, прерыванию его действий и его нейтрализации.

Для успешного реагирования важными факторами являются:

- Наличие точной информации о нарушителе;
- Наличие времени на развертывание сил и средств реагирования;
- Численное превосходство сил СФЗ.

Физическая защита ОИ

Принципы построения эффективной СФЗ:

- **Надежность** (эшелонированность) - наличие нескольких рубежей препятствий, которые должен преодолеть нарушитель;
- **Отказоустойчивость** - наличие запасных мер защиты на случай успеха нарушителя в преодолении основных препятствий;
- **Сбалансированность** - отсутствие явных наиболее простых я преодоления путей достижения цели нарушителем.

Физическая защита ОИ

Принципы построения эффективной СФЗ:

- Обнаружение нарушителя на максимальном удалении от цели;
- Оценка попытки проникновения со стороны нарушителя до завершения его обнаружения;
- Устойчивая связь между обнаружением нарушителя и реагированием на него;
- Задержка обеспечивается на минимально приемлемом удалении от цели.

Защита поддерживающей инфраструктуры

Поддерживающая инфраструктура - комплекс взаимосвязанных обслуживающих структур или объектов, составляющих и (или) обеспечивающих основу функционирования информационной системы

Защита поддерживающей инфраструктуры

Поддерживающая инфраструктура может включать системы:

- электроснабжения;
- теплоснабжения;
- водоснабжения;
- газоснабжения;
- кондиционирования;
- другие системы.

Защита поддерживающей инфраструктуры

Выход из строя какой-либо системы поддерживающей инфраструктуры может привести к:

- Временному прекращению работы ИС;
- Физическому повреждению элементов ИС;
- Повышенному износу элементов ИС;
- Другим нежелательным последствиям.

Защита поддерживающей инфраструктуры

Меры технической безопасности ИС:

- Резервирование систем хранения, обработки и передачи информации;
- Организация системы бесперебойного питания;
- Выбор сертифицированного и качественного аппаратного и программного обеспечения ИС;
- Проведение регламентных работ;
- Поддержка пользователей ИС.