Федеральное государственное образовательное бюджетное учреждение
высшего образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)
Новороссийский филиал

Кафедра «Информатика, математика и общегуманитарные науки»

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

Информационная безопасность компьютерных систем

Направление подготовки: 38.03.05 Бизнес-информатика
Направленность (профиль): ИТ-менеджмент в бизнесе
Программа подготовки: академическая
Форма обучения: заочная
Квалификация (степень) выпускника: Бакалавр

Новороссийск 2019

Тимшина Д.В. Информационная безопасность. Методические рекомендации предназначены для студентов, обучающихся по направлению 38.03.05 «Бизнес-информатика», профиль ИТ-менеджмент в бизнесе (программа подготовки бакалавра, заочная форма обучения) – Новороссийск: Новороссийский филиал Финуниверситета, кафедра «Информатика, математика и общегуманитарные науки», 2019. – 51 с.

Методические рекомендации содержат комплекс требований и методические материалы для освоения дисциплины «Информационная безопасность компьютерных систем».

СОДЕРЖАНИЕ

ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины – формирование у студентов знаний и навыков, связанных с обеспечением защиты информации; творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности объектов информатизации; создание представления об основах информационной безопасности, принципах и методах противодействия несанкционированному информационному воздействию; развитие способностей к логическому и алгоритмическому мышлению.

Задачи дисциплины:

– изучить место и роль информационной безопасности в системе национальной безопасности Российской Федерации; основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные (компьютерные) системы и системы передачи информации;

– сформировать умения и навыки проведения анализа и оценки угроз информационной безопасности объекта;

– обучить работе с современными технологиями обеспечения информационной безопасности;

– сформировать системные представления об управлении информационными рисками;

– изучить методы и средства комплексной защиты информации (информационных ресурсов) в информационных компьютерных системах организаций;

– формирование навыков анализа защищенности компьютерных систем и компонентов ИТ-инфраструктуры организаций.

ЛЕКЦИОННЫЕ МАТЕРИАЛЫ

Сущность информационных рисков. Пока еще не сложилось общепринятого толкования категории «***информационный риск***». Различные **подходы к определению сущности информационных рисков можно классифицировать** по ***основным признакам***:

1) ***по конечному результату риска***;

2) ***по масштабам области применения понятия «информационный риск»***;

3) ***по сущности рисковых событий***.

1) По первому признаку можно выделить ***два подхода***:

- ***1-й подход: информационный риск*** – это возможное событие, в результате которого несанкционированно удаляется, искажается информация, нарушается ее конфиденциальность или доступность. Т.е. понятие информационного риска используется как синоним понятия ***угроза безопасности информации***. Сторонники данного подхода ограничиваются рассмотрением последствий воздействия информационных рисков только на информацию. Данный подход характерен, как правило, для специалистов в области защиты информации.
- ***2-й подход: рассмотрение информационных рисков как экономической категории***. Информационные риски понимаются как случайные события, которые в конечном итоге приводят к возникновению убытков, неполучению прибыли и другим негативным последствиям для предприятия. Такое понимание сущности

информационных рисков соответствует уровню руководства предприятия или владельцев информации.

2) Второй признак классификации позволяет разделить существующие подходы к пониманию информационных рисков ***по степени интеграции объектов, процессов и явлений*** в связи с которыми рассматривается сущность информационных рисков:

- ***информационные риски следует рассматривать только в связи с использованием ИТ***. Здесь под ИТ понимают технологии обработки, хранения и передачи информации с помощью компьютерных систем;

- ***помимо компьютерной безопасности необходимо рассматривать, безопасность систем связи***. Диапазон степени интеграции находится в широких пределах от компьютерных систем до комплексного рассмотрения проблемы, включая информационные риски, связанные с традиционным документооборотом, человеческим фактором, видео и аудио информацией.

3) Третий признак классификации подходов к определению сущности информационных рисков основывается на свойствах информации, утрата которых приводит к информационным рискам. Это требование ***целостности, доступности*** и ***конфиденциальности информации***. В некоторых работах приводится ***требование достоверности.***

Определение понятия «информационный риск» должно показывать сущность информационного риска, связь его с ИС предприятия, последствия воздействия на ИС и предприятие в целом.

Сущность информационного риска в том, что это случайное событие, приводящее к негативным последствиям в ИС. Воздействуя на ИС, риски приводят к убыткам предприятия, в чем и заключается экономический смысл понятия «информационный риск».

Определение (**def**.) информационного риска:

Информационный риск – это возможность наступления случайного события в ИС предприятия, приводящего к нарушению ее функционирования, снижению качества информации, в результате которых наносится ущерб предприятию.

Понятие ***«информационная система***» включает в себя все ресурсы предприятия, которые используются для получения, хранения, обработки, передачи и применения информации, а также ИР.

В ***состав ИС входят следующие компоненты***: компьютерные системы, системы передачи информации, оргтехника, БД и файлы компьютерных систем, документы в печатной форме, аудио и видеоинформация на носителях различной физической природы. В качестве одного из основных ресурсов ИС рассматривается специалист, имеющий отношение к использованию или эксплуатации ИС.

К компьютерным системам относятся компьютеры различного назначения, вычислительные системы и комплексы, вычислительные сети. В качестве компьютерных систем рассматриваются блоки и узлы, входящие в состав других устройств и реализующие программный принцип управления обработкой информации (например: блоки управления станками, транспортными средствами, средствами автоматизированного доступа на объекты, средствами связи и др.).

Важно в определении информационного риска положение о том, что причиной ущерба может служить ***снижение качества информации***. ***Качество информации характеризуется следующими показателями***: достоверность; актуальность; конфиденциальность; полнота; своевременность получения; форма представления; избыточность.

Использование категории «качество информации» в определении информационного риска позволяет существенно расширить рамки рисковых событий и учитывать события, влияющие на все показатели качества информации на всех этапах ее

использования на предприятии, во всех звеньях информационной технологической цепи, включая работу с документами на бумажных носителях, видео и аудио информацией.

Кроме того, следует учитывать специалиста. С одной стороны, специалист - один из основных элементов ИС, противодействующим наступлению инф. рисков. С другой стороны, он является потенциальным источником инф. рисков.

Такой подход к пониманию сущности инф. рисков позволяет руководству предприятия рассматривать проблему противодействия рискам, как ***проблему системную***. Решение ее возможно с привлечением специалистов всех уровней управления и при непосредственном участии первых лиц предприятия.

Приведенное выше определение информационного риска не затрагивает таких негативных явлений, как нарушение авторских прав на использование продукции интеллектуального труда, распространение заведомо ложных сведений о предприятии (дезинформация), неправомочное ограничение доступа к открытой информации, незаконное использование торговой или производственной марки. Т.е., к информационным рискам относятся также события, причины и источники которых находятся во внешней среде и результаты реализации таких событий оказывают влияние, прежде всего, на внешнюю среду предприятия.

(def.) ***Информационный риск – это возможность наступления случайного события, приводящего к нарушениям функционирования ИС предприятия и снижению качества информации, а также к неправомерному использованию, распространению или противодействию распространения информации во внешней среде, в результате которых наносится ущерб предприятию***.

Наиболее полное определение информационного риска вводится с применением понятия ***«информационная сфера предприятия».***

Под информационной сферой предприятия следует понимать ИР, средства и субъекты информационных процессов, а также систему регулирования отношений субъектов информационных процессов во внутренней и внешней среде предприятия.

Следовательно, **(def.)** ***информационный риск – это возможность наступления случайного события в информационной сфере предприятия, в результате которого предприятию будет нанесен ущерб.***

Такая трактовка информационного риска позволяет проследить его влияние на обеспечение основных целей функционирования предприятия – получение максимальной прибыли и достижение стабильности бизнеса. У руководителя появляется возможность оценить информационный риск и, с учетом его опасности для бизнеса, выработать ***адекватную политику управления конкретным риском***.

По определению информационный риск, как и риск любой природы, является случайным событием. Случайный характер инф. риска необходимо учитывать при рассмотрении его сущности и взаимосвязи информационных и экономических рисков.

В соответствии с сущностью процессов, явлений и объектов, порождающих случайности, различают ***объективную и субъективную случайности***. ***Объективная*** - связана с природой материи, ее сущностью. Примеры: броуновское тепловое движение молекул и изменения в генах, приводящие к мутации организмов.

Субъективная случайность определяется неполнотой информации о причинах и сущности случайных событий.

Вывод: принципиальных препятствий предсказания субъективных случайностей не существует. Субъективная случайность перейдет в разряд закономерных событий, если человеку удастся своевременно получить информацию, связанную с этим событием, требуемого качества.

Объективную случайность принципиально невозможно предсказать в силу ее сущности. Используя методы теории вероятностей возможно лишь получить предположительные сведения о случайном событии.

Событие не является случайным для человека, если он своевременно получает качественную информацию. Важной характеристикой события является интервал времени от момента получения информации о рисковом событии до момента наступления этого события. Если необходимая информация получена в момент времени, когда уже невозможно проанализировать ситуацию, принять решение и выполнить необходимые действия до наступления события, то такое событие относится к случайным.

На практике большинство рисковых событий ***относятся к классу субъективных случайных событий***. Например, имея информацию о дефектной детали, невозможно абсолютно точно предсказать время выхода ее из строя и возможные масштабы ущерба. Для этого потребовалось бы собрать и обработать дополнительную информацию, которую в конкретных условиях получить невозможно или экономически нецелесообразно.

Возможность получения всей информации требуемого качества ограничивается отсутствием соответствующих инструментальных средств, методик, времени на сбор и обработку информации, а также отсутствием полных научных знаний о сущности процесса или явления, противодействием конкурентов и злоумышленников.

Для исследования природы информационных рисков важно определить сущность и взаимосвязь понятий: «источник», «причина» и «фактор» риска.

Под ***источником информационных рисков*** понимается субъект, объект, процесс или явление, в котором реализуются причины информационных рисков. Примерами источников информационных рисков: специалист, процесс обработки информации, техническое средство, программа, объекты внешней среды. В зависимости от места расположения и принадлежности источника риска относительно ИС риски делятся на ***внутренние*** и ***внешние.***

Знание источника информационного риска является обязательным для определения причин негативных событий в ИС.

Причиной риска служит явление (событие), вызывающее, обуславливающее риск.

Фактором риска называется состояние процесса или объекта, которое способствует реализации риска.

Причина определяет внутренние источники активности процессов или объектов, порождающих риски. Факторы – обстоятельства, способствующие реализации рисков.

Факторы в меньшей степени связаны с конкретными источниками риска, чем причины рисков. ***Понятию «фактор риска» близко понятие «уязвимость системы», которое используется специалистами по защите информации. Для наступления рискового события необходимо одновременное наличие причины и фактора риска.***

Информационные риски могут быть ***прямые*** и ***косвенные.***

Прямыми считаются риски, в результате которых объекты ИС приходят в неработоспособное состояние. ***Примеры прямых рисков***: утрата работоспособности технических средств в результате отказов, аварий и стихийных бедствий, уничтожение или искажение программных средств, информационных баз данных и т.п.

Информационные риски, которые наносят ущерб предприятию, являющийся следствием воздействия рисков на бизнес-процессы предприятия или внешнюю среду, называются косвенными информационными рисками. Например, при нарушении конфиденциальности информации ухудшается конъюнктура рынка, возможен срыв переговоров с партнерами и другие последствия, приносящие ущерб материальным или интеллектуальным ресурсам предприятия.

Т.о., информационные риски воздействуют на ресурсы ИС, вызывая изменение внутренних и внешних условий функционирования предприятия. В результате предприятие терпит убытки, ему наносится ущерб. Внешние информационные риски

могут напрямую воздействовать на внешнюю среду, в результате чего внешняя среда непосредственно воздействует на бизнес-процессы предприятия.

Любой экономический риск является косвенным информационным риском. Отсутствие качественной информации у ЛПР является причиной экономических рисков.

Прослеживается тесная связь понятий «управление информационными рисками» и «обеспечение экономической безопасности предприятия».

Под «***экономической безопасностью предприятия***» понимается «состояние юридических, экономических отношений, организационных связей, материальных и интеллектуальных ресурсов предприятия, при котором гарантируется стабильность его функционирования, финансово-коммерческий успех, прогрессивное научно-техническое и социальное развитие» (определение дано в толковом словаре).

Резюме. Экономическая безопасность – это состояние предприятия, при котором обеспечивается стабильность и развитие предприятия в условиях возможных рисков. Управление рисками является тем направлением в деятельности руководства предприятия, которое и обеспечивает стабильность и устойчивость предприятия к воздействию возможных рисков.

Экономическая безопасность предприятия достигается путем управления рисками и, прежде всего, информационными рисками. Несмотря на многообразие экономических рисков, их общим свойством является наличие информационной составляющей. Управление этой составляющей сводится к необходимости получения качественной управляющей информации и своевременного ее предоставления ЛПР.

Направления управления информационными рисками. В настоящее время управление рисками исследуется в рамках ***риск-менеджмента***, который является важным направлением науки об управлении. Риск-менеджмент находится в стадии становления и развития. Управление информационными рисками необходимо осуществлять с учетом основных положений ***общего менеджмента***, а также с использованием результатов, полученных в рамках риск-менеджмента.

Концепция управления информационными рисками должна определять основополагающие принципы и идеи, положенные в основу организации управления информационными рисками предприятия. В рамках концепции рассматриваются трактовки основных понятий, ***цели*** и ***задачи управления информационными рисками***, определяются основные ***направления решения этих задач***.

- Определение понятия ***«управление информационными рисками»***:

Под управлением информационными рисками понимается система согласованных мер, мероприятий и процедур, осуществляемых персоналом предприятия с целью минимизации расходов на противодействие информационным рискам и устранение их последствий.

Цель управления информационными рисками – минимизация расходов предприятия на противодействие информационным рискам и ликвидацию последствий их реализации.

Управление информационными рисками предполагает решение следующих задач:

- анализ рисков;
- выработка политики управления информационными рисками;
- оптимизация расходов на управление информационными рисками;
- создание системы управления информационными рисками;
- устранение причин и факторов значимых рисков;
- создание механизмов снижения ущерба от возможных рисков;
- оценка ущерба;
- ликвидация последствий рисковых событий;

- постоянный мониторинг и периодический аудит системы управления рисками;
- анализ эффективности системы управления информационными рисками;
- совершенствование системы управления информационными рисками.

Наиболее ответственная задача: ***анализ информационных рисков***.

1) ***1-й этап анализа***: идентификация информационных рисков, которая заключается в выявлении всех возможных для рассматриваемой информационной системы предприятия (ИСП) рисков и создание их перечня. В процессе идентификации используется ***классификация рисков***. Она позволяет определить место конкретного риска в системе информационных рисков, его природу и потенциальную опасность. Необходимо установить причинно-следственные связи, источники и факторы рисков, механизмы реализации рисков, показатели рисков. По результатам анализа ***делается заключение о значимости информационного риска для предприятия***. ***Значимым*** считается риск, которым нельзя пренебречь при управлении информационными рисками.

Затем под руководством первых лиц предприятия разрабатывается и принимается официальный документ ***программа управления информационными рисками***, которая определяет политику предприятия в области управления рисками, обеспечения качества информации.

В программе управления рисками определяются:

- правовое обеспечение политики управления информационными рисками;
- цели и задачи политики управления информационными рисками;
- характеристика ИС предприятия, внутренней и внешней среды;
- облик системы управления информационными рисками (принципы построения, выполняемые функции, структура);
- задачи структурных подразделений и должностных лиц по управлению информационными рисками;
- порядок мониторинга и аудита системы;
- оценка эффективности системы;
- порядок совершенствования системы.

Реализация программы должна привести к результату: при минимально возможных затратах построена и функционирует система управления инф. рисками, обеспечивающая минимальные расходы на управление инф. рисками.

Перед разработчиками политики управления информационными рисками центральной является ***задача оптимального вложения средств, позволяющая осуществлять управление информационными рисками на требуемом уровне при минимально возможных затратах.***

При решении задачи необходимо руководствоваться следующими ***принципами***:

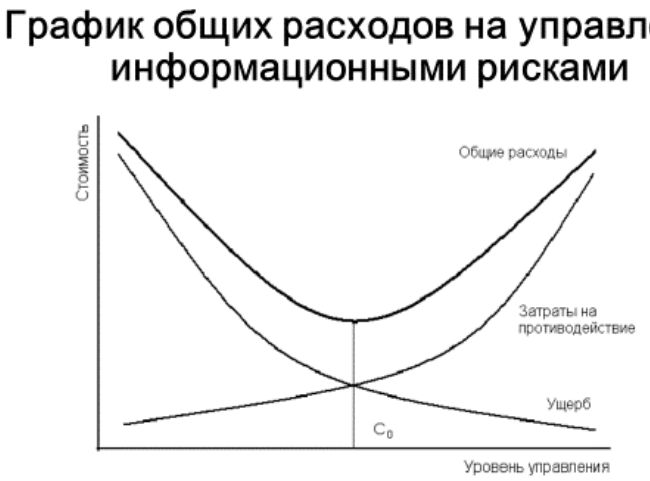
- невозможно создать систему управления информационными рисками, которая позволяла бы обеспечить стопроцентную защиту от рисков;
- защита от рисков осуществляется по направлениям – ***предотвращение возможных рисков*** (приоритетное направление) ***и минимизация ущерба*** (минимизация ущерба достигается своевременностью определения факта наступления рискового события, максимально возможной локализацией воздействия рисков, осуществлением квалифицированного устранения последствий рисковых событий с использованием созданных заблаговременно механизмов);
- с целью минимизации ущерба от рисков применяются специальные механизмы, основанные на временном, информационном, техническом, программном резервировании и резервировании денежных средств (для резервирования денежных средств привлекаются или собственные ресурсы, или осуществляется страхование информационных рисков);

- сложной задачей является оптимальное распределение ресурсов, направляемых на предотвращение информационных рисков и на снижение последствий рисковых событий.

Вложение средств в управление информационными рисками является оптимальным, если сумма затраченных на управление средств и ожидаемых потерь от рисков будет минимальной.

Точка равенства затрат на управление рисками и величины ущерба приведена на слайде:

Слайд



В отношении информационных рисков могут приниматься следующие ***стратегии управления***:

- ***принятие риска*** (в отношении соответствующего риска не применяются никакие механизмы предотвращения информационного риска и минимизации ущерба от его реализации. Стратегия выбирается в отношении рисков, ожидаемый ущерб от которых незначителен; при очень малой вероятности рискового события и ожидаемом ущербе, который не относится к категории катастрофических);
- ***предотвращение риска*** (Стратегия предполагает воздействие на источники рисков с целью снижения вероятности наступления рискового события и требует устранения факторов, способствующих реализации рисков.);
- ***снижение возможного ущерба от риска*** (Величина ущерба от риска может быть снижена, если заблаговременно внедряются специальные механизмы. Суть принимаемых мер - в придании устойчивости предприятия к воздействию рисков. ***Основа такой стратегии - адаптивная система управления и необходимые резервные ресурсы***: аппаратные, программные, информационные и финансовые);
- ***предотвращение риска и снижение возможного ущерба от него.***

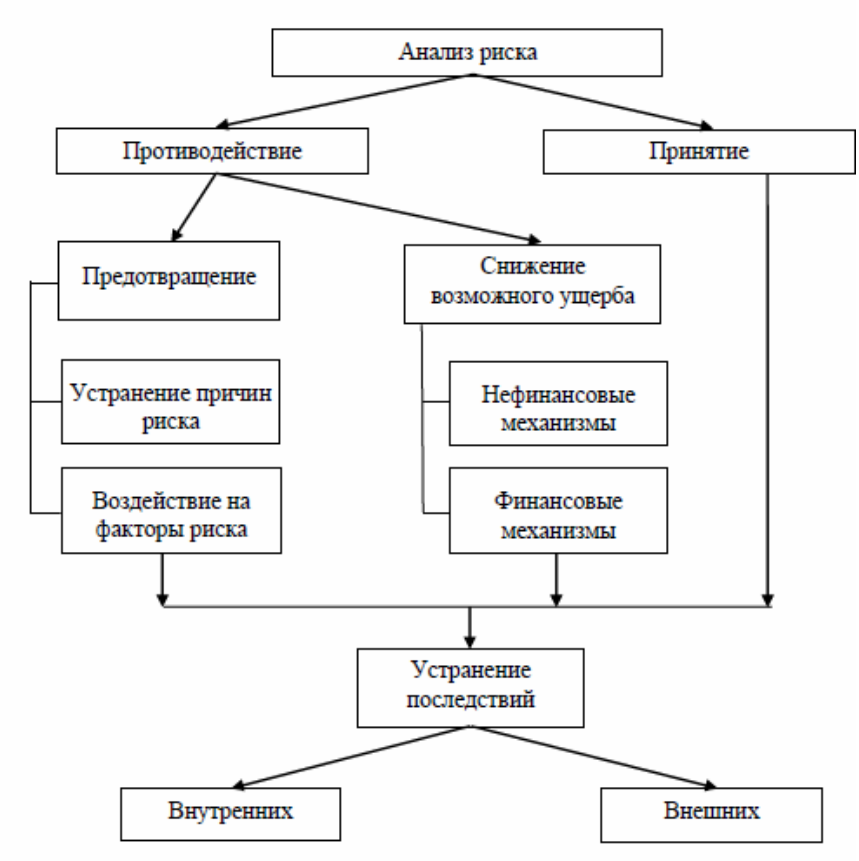
Резюме

Наиболее совершенная стратегия предполагает использование механизмов предотвращения информационных рисков и механизмов снижения ущерба от них.

Процесс управления информационными рисками представим в виде схемы:

Слайд

Схема управления информационными рисками с учетом выбора стратегии



Анализ информационных рисков. ***Цель проведения анализа информационных рисков*** – получение наиболее полных характеристик информационных рисков, которые могут нанести существенный вред предприятию и, вероятность наступления которых не позволяет пренебречь ими. Такие риски называются ***значимыми***.

Для полного и всестороннего анализа информационных рисков необходимо использовать ***методологию системного исследования явлений***.

Данный подход представлен в виде следующей последовательности действий:

- идентификация информационных рисков;
- определение механизма воздействия информационных рисков на ИС;
- выявление источников, факторов рисков и причин их порождающих;
- определение взаимосвязи информационных рисков;
- классификация рисков;
- выбор показателей оценки рисков;
- выбор методов и средств оценки рисков;
- оценка рисков.

Анализ рисков начинается с ***построения информационной модели предприятия***. Модель должна включать: подробный перечень информационных объектов, выполняемых объектами функций, связей объектов; сведения о внутренних и внешних информационных потоках, об особенностях информации, степени ее важности и статусе (конфиденциальная или открытая); сведения о взаимодействии ИС предприятия с внешними системами и с бизнес-процессами предприятия. Модель предприятия должна отражать особенности всех режимов функционирования ИС, возможные изменения внешней среды и смежных систем.

На этапе выявления факторов рисков информационная модель предприятия может быть представлена с использованием схем взаимодействия, алгоритмов функционирования, графов и таблиц.

Построение системы управления информационными рисками. Составление полного перечня возможных информационных рисков предполагает выполнение следующих мероприятий.

В информационной модели выделяются типовые информационные объекты: рабочее место специалиста, телефонная сеть, технические средства хранения информации, специалист конкретного профиля и уровня компетентности и т.д.

Структурируются информационные процессы ИС по стадиям получения, обработки, хранения и передачи информации, по уровням иерархии, по важности информации.

Специалист-аналитик включает в список возможных рисков предприятия те, которые потенциально могут иметь место в конкретной ИС для каждого типового информационного объекта и процесса. Полные списки возможных рисков специалист получает по результатам собственных исследований, обследований, из научно-технической литературы, стандартов, методических рекомендаций.

***Под* механизмом воздействия информационного риска на ИС *понимается физический принцип, лежащий в основе явлений и процессов, которые могут привести к реализации риска, алгоритмы, методы и средства реализации риска*.**

Одна из основных задач анализа рисков - ***установление причинно-следственных связей***, лежащих в основе информационных рисков.

Программа управления информационными рисками содержит все данные, необходимые для построения системы управления информационными рисками.

Под системой управления информационными рисками (СУИР) ***понимается единый комплекс правовых норм, экономических и организационных мер, технических, программных и криптографических средств, а также ИР, обеспечивающий минимальные суммарные расходы на предотвращение информационных рисков и компенсацию ущерба от них*.**

Система управления информационными рисками является одной из подсистем ИС предприятия и должна создаваться на единых с ИС предприятия ***научно-методических принципах построения сложных человеко-машинных систем*.**

Такими принципами являются:

- системный подход;
- непрерывность функционирования;
- равнозащищенность всех звеньев;
- принцип многоуровневой защиты;
- адаптивность системы;
- централизованное иерархическое управление;
- дружественный интерфейс;
- открытость системы.

Принцип системности требует:

- учета при построении системы всех возможных информационных рисков;
- управления информационными рисками на всех жизненных циклах ИСП;
- управления информационными рисками во всех звеньях и на всех уровнях ИСП;
- учета взаимодействия с другими системами и внешней средой;
- комплексного согласованного использования методов и средств управления информационными рисками.

При создании СУИР необходимо анализировать все возможные виды информационных рисков для конкретной ИСП. На основе полученной информации осуществляется выбор адекватных мер и средств предотвращения рисков или снижения вероятности их реализации, а также устранения последствий рисков.

За время своего существования ИС предприятия и ее отдельные объекты проходят несколько этапов или жизненных циклов: ***создание, использование, модернизация,***

утилизация технических средств, ликвидация организационной структуры. Управление информационными рисками ведется на всех этапах постоянно, включая переходные периоды.

На всем технологическом пути перемещения информации в ИС ***необходимо обеспечивать ее качество***. По мере продвижения от источников к верхним уровням управления значимость информации возрастает, что и должно учитываться при построении СУИР.

При построении СУИР исследуются все объекты, с которыми взаимодействует ИСП внутри предприятия и за его пределами. Связи СУИР с другими объектами должны быть максимально структурированными и по возможности формализованы.

Невозможно построить СУИР, используя отдельные методы и средства управления информационными рисками. ***Правовые и организационные методы управления являются приоритетными, т.к. обеспечивают комплексное правовое использование всех других методов и средств.***

СУИР должна функционировать постоянно и в ней необходимо обеспечить единый уровень защищенности информации от рисков во всех звеньях. Наличие ***слабого звена*** исключает возможность построения надежной сбалансированной СУИР. Степень защищенности ИСП от воздействия рисков должна определяться возможностями противодействия рискам в наименее защищенном звене.

Повышение эффективности СУИР достигается за счет создания ***многоуровневой защиты.***

Чем выше значимость информации, тем большее число уровней противодействия рискам должно быть задействовано.

Уровни защиты называются также ***рубежами защиты.***

Например, для защиты информации от несанкционированного доступа в автономной компьютерной системе могут использоваться следующие рубежи: рубеж контролируемой территории, рубеж здания, рубеж помещения, рубеж технического устройства, программный рубеж, рубеж информационного массива (базы данных).

СУИР должна обеспечивать устойчивость ИСП к воздействию информационных рисков. Требуемую устойчивость может обеспечить только ***адаптивная система***. Для решения этой задачи ИС предприятия необходимо иметь определенную избыточность, которая позволяла бы выполнять следующие задачи:

- постоянный мониторинг системы;
- определение и локализация рисков;
- оценка последствий реализации риска;
- реконфигурация системы, включая и человеческие ресурсы;
- обеспечение функционирования системы в условиях реализованного риска, возможно и с ухудшенными характеристиками;
- восстановление объектов, поврежденных или утраченных ресурсов;
- обратная реконфигурация системы, для работы в штатном режиме;
- ликвидация последствий воздействия рисков на бизнес-процессы предприятия.

Однако, возможности любой адаптивной системы ограничены, она может обеспечить работоспособность ИСП только в определенных границах. Возможны ситуации, когда системе наносится такой урон, при котором механизмы адаптации не могут компенсировать нанесенный ущерб.

Преимущество адаптивных систем перед другими системами: обеспечивают максимально возможное использование всех ресурсов в условиях отсутствия рисков. При наступлении рисковых событий часть ресурсов направляется на компенсацию ущерба. Высокая степень автоматизации процессов адаптации и выбор оптимальных процедур реконфигурации системы позволяют своевременно локализовать распространение влияния негативных событий.

В человеко-машинных системах самое активное участие в компенсаторных механизмах принимает ***человек*** и использует весь комплекс восстановительных механизмов, в том числе ***организационные*** и ***экономические меры***.

Одним из важных принципов, лежащих в основе построения СУИР, является создание ***централизованного иерархического управления***. Без которого невозможна эффективная реализация единой политики управления информационными рисками. Роль централизации управления возрастает на предприятиях, которые имеют удаленные филиалы, дочерние компании. Практическая реализация централизованного управления на данных предприятиях требует решения целого ряда сложных технических и организационных проблем.

Иерархический принцип управления позволяет построить оптимальную систему, в которой исключены потоки информации, не соответствующие уровню компетентности органа управления. На верхние уровни управления попадает информация, прошедшая соответствующую обработку и обобщение на низших уровнях.

Многие вопросы управления информационными рисками решаются на отраслевом и государственном уровне. ***Законы, стандарты и концепции, ведомственные руководящие документы и инструкции, обязательное лицензирование и сертификация позволяют государству оказывать значительное воздействие на процессы управления информационными рисками на предприятиях с любым видом собственности***.

СУИР предполагает выполнение сотрудниками определенных обязанностей, которые требуют регулярного и точного выполнения. Если эти обязанности излишне обременительны, то у человека может появиться желание отказа от выполнения отдельных обязательных операций. Для решения этой проблемы СУИР должна обеспечивать дружественный интерфейс системы с сотрудниками предприятия.

Под ***дружественным интерфейсом*** понимается безопасное и комфортное взаимодействие человека с системой, при котором достигается максимальная производительность человеко-машинной системы и ее защищенность от информационных рисков. Дружественный интерфейс позволяет сократить количество неумышленных ошибок персонала, способствует выполнению специалистами своих обязанностей по защите от информационных рисков.

Принцип открытости предполагает выбор такой архитектуры системы, которая позволяла бы наращивать возможности системы для парирования вновь появляющихся информационных рисков. Открытая система должна иметь запас ресурсов, которые могут быть использованы при модернизации системы.

Блочный принцип построения с использованием стандартных интерфейсов и правильных конструктивных решений позволяют легко заменять блоки более мощными или подключать дополнительные блоки.

Правовое регулирование в области безопасности информации. Правовые методы защиты информации служат основой легитимного (законного) построения ИС и использования информации, создания систем защиты ИС.

В масштабах страны обеспечение ИБ осуществляет государство, которое создает необходимые условия в стране для безопасного использования современных ИТ в интересах государственных органов, различных организаций и отдельных граждан.

Чтобы решить эту проблему государство должно:

1) ***выработать государственную политику безопасности*** в области ИТ;

2) ***законодательно определить правовой статус компьютерных технологий***, компьютерных систем, информации, систем защиты информации, владельцев и пользователей информации и т. д.;

3) ***создать структуру государственных органов***, вырабатывающих и проводящих в жизнь политику безопасности информационных технологий;

4) ***создать систему стандартизации и технического регулирования, лицензирования и сертификации в области защиты информации***;

5) обеспечить приоритетное развитие отечественных защищенных ИТ;

6) ***повышать уровень образования граждан в области ИТ и обеспечения ИБ***, воспитывать у них патриотизм и бдительность;

7) обеспечить ***свободный доступ граждан к открытой информации***;

8) ***оградить граждан страны от информации, распространение которой запрещено нормативными правовыми актами РФ***;

9) ***установить ответственность граждан за нарушения законодательства в области ИТ***.

Решение этих масштабных задач требует от государства разработать и претворять в жизнь государственную политику по обеспечению безопасности ИТ на всех уровнях и во всех сферах человеческой деятельности.

- В РФ ***вопросы ИБ*** впервые нашли отражение в ***«Концепции национальной безопасности Российской Федерации»***, утвержденной Указом Президента РФ № 1300 от 17 декабря 1997 г. В документе отмечается, что «в современных условиях всеобщей информатизации и развития ИТ резко возрастает значение обеспечения национальной безопасности РФ в информационной сфере».
- Указом Президента Российской Федерации № Пр-1895 от 9 сентября 2000 г. утверждена «Доктрина информационной безопасности Российской Федерации». Доктрина развивает Концепцию национальной безопасности РФ применительно к информационной сфере.

Доктрина ИБ РФ - совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения ИБ РФ.

В Доктрине отмечается, что она служит основой для:

• ***формирования государственной политики в области обеспечения*** ИБ РФ;

• ***подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения*** ИБ РФ;

• ***разработки целевых программ обеспечения ИБ РФ.***

В Доктрине подчеркивается роль информационной сферы, которая представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Информационная сфера активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности РФ. Национальная безопасность РФ существенным образом зависит от обеспечения ИБ.

Под ***информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства***.

- ***Интересы личности в информационной сфере*** заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.
- ***Интересы общества в информационной сфере*** заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.
- ***Интересы государства в информационной сфере*** заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и

гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

На основе ***национальных интересов*** РФ в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению ИБ.

Основные ***составляющие национальных интересов РФ*** в информационной сфере:

I. Первая составляющая включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Для достижения этого требуется:

1) повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа РФ;

2) усовершенствовать систему формирования, сохранения и рационального использования ИР, составляющих основу научно-технического и духовного потенциала РФ;

3) обеспечить ***конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом***, получать ***достоверную информацию о состоянии окружающей среды***;

4) обеспечить ***конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений***, на защиту своей чести и своего доброго имени;

5) укрепить механизмы правового регулирования отношений в области ***охраны интеллектуальной собственности***, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;

6) гарантировать ***свободу массовой информации и запрет цензуры***;

7) ***не допускать пропаганду и агитацию***, которые способствуют ***разжиганию социальной, расовой, национальной или религиозной ненависти и вражды***;

8) обеспечить ***запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия*** и другой информации, доступ к которой ограничен федеральным законодательством.

II. Вторая составляющая включает в себя ***информационное обеспечение государственной политики РФ***, связанное с доведением до российской и международной общественности достоверной информации о государственной политике РФ, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным ИР.

Для достижения этого требуется:

1) ***укреплять государственные средства массовой информации***, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;

2) интенсифицировать формирование открытых государственных ИР, повысить эффективность их хозяйственного использования.

III. Третья составляющая включает в себя ***развитие современных ИТ***, отечественной индустрии информации, в том числе индустрии ***средств информатизации, телекоммуникации и связи***, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок; обеспечение накопления, сохранности и эффективного использования отечественных ИР. На этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. ***Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности***.

Для достижения этого требуется:

1) ***развивать*** и совершенствовать ***инфраструктуру единого информационного пространства РФ***;

2) ***развивать отечественную индустрию информационных услуг*** и ***повышать*** эффективность использования государственных ИР;

3) ***развивать производство*** в РФ ***конкурентоспособных средств и систем информатизации, телекоммуникации и связи***, расширять участие России в международной кооперации производителей этих средств и систем;

4) ***обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи***.

IV. Четвертая составляющая национальных интересов Российской Федерации в информационной сфере включает защиту ИР от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, уже развернутых и создаваемых на территории России.

В этих целях необходимо:

1) повысить безопасность ИС, включая сети связи, безопасность первичных сетей связи и ИС федеральных органов государственной власти, органов государственной власти субъектов РФ, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности; систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;

2) ***интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации*** и методов контроля за их эффективностью;

3) ***обеспечить защиту сведений, составляющих государственную тайну***;

4) расширять международное сотрудничество РФ в области развития и безопасного использования ИР, противодействия угрозе развязывания противоборства в информационной сфере.

В Доктрине дан обстоятельный анализ:

1) ***внутренних и внешних угроз*** ИБ РФ, угроз безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России;

2) ***источников угроз*** ИБ РФ;

3) информационной безопасности РФ и приведены основные задачи по ее обеспечению.

В Доктрине раскрывается ***сущность государственной политики обеспечения информационной безопасности РФ.***

Государственная политика обеспечения ИБ РФ определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов РФ в этой области, порядок закрепления их обязанностей по защите интересов РФ в информационной сфере в рамках направлений их деятельности и

базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

- В Доктрине рассматриваются ***особенности обеспечения ИБ РФ в различных сферах общественной жизни*** (в области экономики, во внутренней политике, во внешней политике, в науке и технике, духовной жизни, в общегосударственных информационных и телекоммуникационных системах, в сфере обороны, в правоохранительной и судебной сферах).
- Рассматривается в Доктрине ***организационная основа системы обеспечения информационной безопасности РФ.***

Для достижения ***целей политики обеспечения ИБ*** государство создает необходимую ***нормативную правовую базу***. Ее можно представить в виде ***иерархической системы нормативных правовых актов.***

На ***верхнем уровне*** регулируются ***основы ИБ государства, предприятия и гражданина РФ***, а также вопросы комплексной защиты информации, имеющие отношение ко всем направлениям обеспечения ИБ.

К ***нормативным правовым актам этого уровня*** относятся: «Конституция Российской Федерации»; «О безопасности» от 5.03.1992 № 2446-1; «Об информации, информационных технологиях и о защите информации» от 27.07.06 № 149-ФЗ; «О техническом регулировании» от 27.12.2002 № 184-ФЗ.

ФЗ «Об информации, информационных технологиях и о защите информации» - базовый федеральный закон РФ, регулирующий правоотношения в информационной сфере государства. Значение этого закона заключается, в определении основных понятий ***информационного права***. В законе определены такие термины как: ***информация, информационные технологии, обладатель информации, конфиденциальность информации*** и др.

В законе закреплены основы политики государства в сфере ИТ, права и обязанности субъектов информационного права, а также принципы регулирования ответственности за правонарушения в информационной сфере.

Следующий уровень составляют законы, развивающие и конкретизирующие положения информационного права применительно к определенным областям информационной безопасности.

К ним относятся действующие законы: «О государственной тайне» от 21.07.1993 № 5485-1; «О коммерческой тайне» от 29.07.2004 № 98-ФЗ; «О связи» от 07.06.2003 № 126-ФЗ; «О средствах массовой информации» от 27.12.1991 № 2124-I; «О рекламе» от 13.03.2006 № 38-ФЗ; «О персональных данных» от 27.07.06 №152 – ФЗ и др.

Эта группа законов ***вводит новые дефиниции в конкретной сфере информационного права.*** Законы регулируют взаимоотношения субъектов права при работе с определенного вида информацией (персональной информацией, информацией, составляющей государственную или коммерческую тайну), при использовании информационных технологий для реализации определенных бизнес-процессов (передачи информации по каналам связи, массового распространения информации, рекламе, электронной торговле и т. д.).

К третьему самому низкому уровню иерархии законов относятся законы, которые ***регламентируют применение определенного механизма противодействия информационным рискам.*** Например, ФЗ «Об электронной подписи» от 06.04.2011 № 63-ФЗ.

Для технологий, являющихся наиболее важными при обеспечении ИБ государства, применяется регулирование в рамках ***отдельного закона.***

Особое место в вопросах обеспечения ИБ занимают ***кодифицированные законы РФ***: «Гражданский кодекс Российской Федерации (часть четвертая)» от 18.12.2006 № 230-ФЗ; «Кодекс Российской Федерации об административных правонарушениях» от

13.12.2001 № 195-ФЗ; «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ; «Трудовой кодекс Российской Федерации» от 30.12.2001 № 197-ФЗ и др. акты.

Кодифицированные законы содержат отдельные главы и статьи, регулирующие отношения в информационной сфере, в т.ч. определяющие ответственность граждан за нарушения информационного законодательства.

Следующий уровень нормативного правового регулирования общественных отношений в информационной сфере составляют ***законы субъектов РФ, подзаконные акты органов государственного управления и местного самоуправления***. Наиболее важные вопросы развития положений законов РФ отражаются в ***указах и распоряжениях Президента РФ*** и в ***постановлениях Правительства РФ***.

Стандарты как механизм управления информационными рисками. Система стандартов позволяет решать следующие задачи управления информационными рисками:

• согласование характеристик блоков, устройств, систем и процессов для их эффективного бесконфликтного совместного использования;

• обеспечение сравнимости результатов измерений и исследований, технических и экономико-статистических данных;

• оценка эффективности функционирования системы или качества продукта;

• определение уровня соответствия объекта исследования лучшим мировым или национальным образцам;

• взаимозаменяемость средств информатизации и ИТ;

• сертификация и лицензирование в сфере информационной безопасности.

Стандарты управления информационными рисками могут быть распределены по трем иерархическим уровням:

- на ***верхнем уровне*** иерархии стандартов находятся ***стандарты, предназначенные для эффективного использования ИС и ИТ***. Стандарты позволяют повысить устойчивость бизнеса и его эффективность за счет внедрения новых ИТ. Информационные риски связываются не только с ***нарушением безопасности***, но и со ***снижением качества информации ниже приемлемого уровня***.

Наиболее известные стандарты этого уровня:

- отраслевой стандарт США Control Objectives for Information and related Technology (**CobiT**);
- отраслевой стандарт IT Infrastructure Library (**ITIL**) (наиболее часто используется в Великобритании, Нидерландах и Австралии);
- национальный стандарт Великобритании **BS 15000**.

Наибольшую популярность получил стандарт ***CobiT, который стал de facto международным стандартом управления информационными технологиями.*** В стандарте отмечается, что «…главной целью проекта CobiT является развитие четкой политики и оптимальных систем безопасности и контроля информационных технологий с последующим широким применением в коммерческих, правительственных и профессиональных организациях. Развитие объектов контроля предусмотрено, в первую очередь, с точки зрения производственных целей и нужд…». Т.е. во главу угла процесса управления ИТ ставится задача оптимизации бизнес-процессов, нацеленность на конечный результат использования ИС – повышение эффективности, безопасности и надежности бизнеса.

Стандарт CobiT рассчитан на использование менеджерами предприятия, пользователями ИС и аудиторами. Стандарт активно совершенствуется.

На высшем уровне иерархии стандартов находится ряд стандартов, которые дополняют рассмотренные стандарты.

К ним относятся:

- **стандарты аудита ISO 19011, SAC, COSO, SAS**;

- **стандарты управления качеством ISO 9001, EFQM** и др.

Второй уровень в иерархии стандартов составляют ***стандарты управления системами информационной безопасности и качеством информации.*** Эти стандарты определяют процессы создания, эксплуатации, модернизации и утилизации систем информационной безопасности и систем управления информационными рисками.

Стандарты определяют требования к системам, рассматривая их на системном уровне как организационно-техническую систему; вводят терминологию, определяют требования по организации процессов создания и функционирования систем, порядок подтверждения характеристик систем требованиям стандартов, обеспечивают возможность оценки эффективности систем и их сравнимость для выбора оптимального варианта системы.

Примеры стандартов:

- международные стандарты управления информационной безопасностью семейства ***ISO 27000*** (более 20 стандартов);
- **ГОСТ Р ИСО/МЭК ТО 18044** «Информационная технология. Методы обеспечения безопасности. Руководство по менеджменту безопасностью информации»;
- **ГОСТ Р ИСО/МЭК 18045** «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»;
- **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;
- **ГОСТ Р ИСО/МЭК 18028-1** «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Часть 1. Менеджмент сетевой безопасности»;
- **ГОСТ Р ИСО/ТО 13569-2007.** Финансовые услуги. Рекомендации по информационной безопасности;
- **ГОСТ 17799-2005 (ISO 17799:2005)**. Практические правила управления информационной безопасностью;
- **ГОСТ Р ИСО/МЭК 15408-2002.** Критерии оценки безопасности информационных технологий;
- **ГОСТ Р 51169-98.** Качество служебной информации. Система сертификации информационных технологий в области качества служебной информации. Термины и определения;
- **ГОСТ Р 52294-2004.** Информационная технология. Управление организацией. Электронный регламент административной и служебной деятельности. Основные положения;
- **ГОСТ РВ 51987 ИТ.КСАС.** Требования и показатели качества функционирования информационных систем. Общие положения;
- **ГОСТ Р 50739-95.** Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России;
- **ГОСТ Р 50922-96.** Защита информации. Основные термины и определения. Госстандарт России;
- **ГОСТ Р 51188-98.** Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России;
- **ГОСТ Р 51275-99.** Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России.

На ***третьем уровне*** находятся стандарты, которые ***определяют алгоритмы, принципы действия, порядок применения определенных механизмов защиты и***

***защищенных ИТ и требования к процессам создания и эксплуатации механизмов защиты*.**

К стандартам этого уровня относятся:

- стандарты шифрования с симметричными ключами DES и AES (США), ГОСТ 28147-89 (Россия);
- стандарт шифрования с открытыми ключами RSA;
- стандарты цифровой подписи DSS (США) и ГОСТ Р 34.10 – 94 (Россия);
- стандарт использования хэш-функции;
- RAID технология – стандарт de facto, определяющий организацию надежного и эффективного хранения данных и др.

Стандарты в области ИБ дополняются ***нормативными и методическими документами Государственной технической комиссии и Федеральной службы технического и экспортного контроля, например*:**

- Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30.03.1992;
- Руководящий документ. Защита от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30.03.1992;
- Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30.03.1992;
- Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 25.07.1997;
- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Приказ председателя Гостехкомиссии России от 19.06.2002 № 1;
- Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003 год;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год и проч.

Угрозы информационной безопасности. Классификация угроз информационной безопасности. Терминология и подходы к классификации. Организация обеспечения безопасности информации должна носить комплексный характер и основываться на глубоком анализе возможных негативных последствий, который предполагает обязательную идентификацию возможных источников угроз, факторов, способствующих их проявлению и, как следствие, определение актуальных угроз безопасности информации.

В ходе анализа необходимо убедиться, что все возможные источники угроз идентифицированы, идентифицированы и сопоставлены с источниками угроз все возможные факторы (уязвимости), присущие объекту защиты, всем идентифицированным источникам и факторам сопоставлены угрозы безопасности информации.

Исходя из данного принципа, классификацию источников угроз и их проявлений, целесообразно проводить на основе анализа взаимодействия логической цепочки: **источник угрозы - фактор (уязвимость) - угроза (действие) - последствия (атака).**

Источник угрозы - это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

Угроза (действие) - это возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения и потери информации.

Фактор (уязвимость) - это присущие объекту информатизации причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми ПО и аппаратной платформой, условиями эксплуатации.

Последствия (атака) - это возможные последствия реализации угрозы (возможные действия) при взаимодействии источника угрозы через имеющиеся факторы (уязвимости).

Атака - это всегда пара ***«источник – фактор***», реализующая угрозу и приводящая к ущербу. Анализ последствий предполагает проведение анализа возможного ущерба и выбора методов парирования угроз безопасности информации.

Угроза, как следует из определения, это опасность причинения ущерба, т.е. в этом определении проявляется жесткая связь технических проблем с юридической категорией, каковой является «ущерб».

Классификация угроз информационной безопасности. Угрозами безопасности информации являются:

- хищение (копирование) информации;
- уничтожение информации;
- модификация (искажение) информации;
- нарушение доступности (блокирование) информации;
- отрицание подлинности информации;
- навязывание ложной информации.

Классификация источников угроз. Носителями угроз безопасности информации являются источники угроз. В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления. Источники угроз могут находиться как внутри защищаемой организации - внутренние источники, так и вне ее - внешние источники. Деление источников на субъективные и объективные оправдано исходя из предыдущих рассуждений по поводу вины или риска ущерба информации. А деление на внутренние и внешние источники оправдано потому, что для одной и той же угрозы методы парирования для внешних и внутренних источников могу быть разными.

Все источники угроз безопасности информации можно разделить на три основные группы:

I. ***Обусловленные действиями субъекта*** (антропогенные источники угроз).
II. ***Обусловленные техническими средствами*** (техногенные источники угрозы).
III. ***Обусловленные стихийными источниками***.

Антропогенные источники угроз. Антропогенными источниками угроз безопасности информации выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления.

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Субъекты (источники), действия которых

могут привести к нарушению безопасности информации могут быть как внешние, так и внутренние.

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся: криминальные структуры; потенциальные преступники и хакеры; недобросовестные партнеры; технический персонал поставщиков услуг; представители надзорных организаций и аварийных служб; представители силовых структур.

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации ПО и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями, и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся: основной персонал (пользователи, программисты, разработчики); представители службы защиты информации; вспомогательный персонал (уборщики, охрана); технический персонал (жизнеобеспечение, эксплуатация).

Особую группу внутренних антропогенных источников составляют лица с нарушенной психикой и специально внедренные и завербованные агенты, которые могут быть из числа основного, вспомогательного и технического персонала, а также представителей службы защиты информации. Данная группа рассматривается в составе перечисленных выше источников угроз, но методы парирования угрозам для этой группы могут иметь свои отличия.

Квалификация антропогенных источников информации играют важную роль в оценке их влияния и учитывается при ранжировании источников угроз.

Техногенные источники угроз. Вторая группа содержит источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Однако, последствия, вызванные такой деятельностью вышли из-под контроля человека и существуют сами по себе. Эти источники угроз менее прогнозируемые, напрямую зависят от свойств техники и поэтому требуют особого внимания. Технические средства, являющиеся источниками потенциальных угроз безопасности информации, так же могут быть внешними: средства связи; сети инженерных коммуникации (водоснабжения, канализации); транспорт и внутренними: некачественные технические средства обработки информации; некачественные программные средства обработки информации; вспомогательные средства (охраны, сигнализации, телефонии); др. технические средства.

Стихийные источники угроз. Третья группа источников угроз объединяет, обстоятельства, составляющие непреодолимую силу, т. е. обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. К непреодолимой силе в законодательстве относят стихийные бедствия или иные обстоятельства, которые невозможно предусмотреть или предотвратить, или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей.

Такие источники угроз совершенно не поддаются прогнозированию и поэтому меры защиты от них должны применяться всегда.

Стихийные источники потенциальных угроз информационной безопасности как правило являются внешними по отношению к защищаемому объекту и под ними понимаются прежде всего природные катаклизмы: пожары; землетрясения; наводнения; ураганы; различные непредвиденные обстоятельства; необъяснимые явления; другие форс-мажорные обстоятельства.

Классификация уязвимостей безопасности. Угрозы, как возможные опасности совершения какого-либо действия, направленного против объекта защиты, проявляются не сами по себе, а через уязвимости (факторы), приводящие к нарушению безопасности информации на конкретном объекте информатизации.

Уязвимости присущи объекту, неотделимы от него и обуславливаются недостатками процесса функционирования, свойствами архитектуры автоматизированных систем, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации и расположения.

Источники угроз могут использовать уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации). Возможно не злонамеренные действия источников угроз по активизации тех или иных уязвимостей, наносящих вред.

Каждой угрозе могут быть сопоставлены различные уязвимости. Устранение или существенное ослабление уязвимостей влияет на возможность реализации угроз безопасности информации.

Для удобства анализа, уязвимости разделены на классы, группы и подгруппы. Уязвимости безопасности информации могут быть: объективными, субъективными, случайными.

Объективные уязвимости. Объективные уязвимости зависят от особенностей построения и технических характеристик оборудования, применяемого на защищаемом объекте. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-техническими методами парирования угроз безопасности информации. К ним можно отнести:

- сопутствующие техническим средствам излучения:

- электромагнитные (побочные излучения элементов технических средств, кабельных линий технических средств, излучения на частотах работы генераторов, на частотах самовозбуждения усилителей)
- электрические (наводки электромагнитных излучений на линии и проводники, просачивание сигналов в цепи электропитания, в цепи заземления, неравномерность потребления тока электропитания)
- звуковые (акустические, виброакустические)

- активизируемые:

- аппаратные закладки (устанавливаемые в телефонные линии, в сети электропитания, в помещениях, в технических средствах)
- программные закладки (вредоносные программы, технологические выходы из программ, нелегальные копии ПО)

- определяемые особенностями элементов:

- элементы, обладающие электроакустическими преобразованиями (телефонные аппараты, громкоговорители и микрофоны, катушки индуктивности, дроссели, трансформаторы и пр.)
- элементы, подверженные воздействию электромагнитного поля (магнитные носители, микросхемы, нелинейные элементы, поверженные ВЧ навязыванию)

- определяемые особенностями защищаемого объекта:

- местоположением объекта (отсутствие контролируемой зоны, наличие прямой видимости объектов, удаленных и мобильных элементов объекта, вибрирующих отражающих поверхностей)
- организацией каналов обмена информацией (использование радиоканалов, глобальных информационных сетей, арендуемых каналов).

Субъективные уязвимости. Субъективные уязвимости зависят от действий сотрудников и, в основном, устраняются организационными и программно-аппаратными методами:

- ошибки:

- при подготовке и использовании программного обеспечения (при разработке алгоритмов и программного обеспечения, инсталляции и загрузке программного обеспечения, эксплуатации программного обеспечения, вводе данных)
- при управлении сложными системами (при использовании возможностей самообучения систем, настройке сервисов универсальных систем, организации управления потоками обмена информации)
- при эксплуатации технических средств (при включении/ выключении технических средств, использовании технических средств охраны, использовании средств обмена информацией)

- нарушения:

- режима охраны и защиты (доступа на объект, доступа к техническим средствам)
- режима эксплуатации технических средств (энергообеспечения, жизнеобеспечения)
- режима использования информации (обработки и обмена информацией, хранения и уничтожения носителей информации, уничтожения производственных отходов и брака)
- режима конфиденциальности (сотрудниками в нерабочее время, уволенными сотрудниками).

Случайные уязвимости. Случайные уязвимости зависят от особенностей окружающей защищаемый объект среды и непредвиденных обстоятельств. Эти факторы, как правило, мало предсказуемы и их устранение возможно только при проведении комплекса организационных и инженерно-технических мероприятий по противодействию угрозам информационной безопасности:

- сбои и отказы:

- отказы и неисправности технических средств (обрабатывающих информацию, обеспечивающих работоспособность средств обработки информации, обеспечивающих охрану и контроль доступа)
- старение и размагничивание носителей информации (съемных носителей, жестких дисков, элементов микросхем, кабелей и соединительных линий)
- сбои ПО (операционных систем и СУБД, прикладных программ, сервисных программ, антивирусных программ)
- сбои электроснабжения (оборудования, обрабатывающего информацию, обеспечивающего и вспомогательного оборудования)

- повреждения:

- жизнеобеспечивающих коммуникаций (электро-, водо-, газо-, теплоснабжения, канализации, кондиционирования и вентиляции)
- ограждающих конструкций (внешних ограждений территорий, стен и перекрытий зданий, корпусов технологического оборудования).

Классификация угроз информационной безопасности.

По источникам происхождения:

• ***природного происхождения*** - это опасные геологические, метеорологические, гидрологические явления, деградацию почв недр, природные пожары, массовое разрушение (через природные катаклизмы) каналов связи, изменение состояния водных ресурсов и биосферы и тому подобное;

• ***техногенного происхождения*** - транспортные аварии (катастрофы), пожары, неспровоцированные взрывы или их угроза, внезапное разрушение каналов связи, аварии на инженерных сетях и сооружениях жизнеобеспечения, аварии главных серверов системы управления национальной безопасностью и т. п.;

• ***антропогенного происхождения*** - совершение человеком различных действий по разрушению информационных систем, ресурсов, ПО и т. д.

В этой группе по содержанию действий относятся: непреднамеренные, вызванные ошибочными или непреднамеренными действиями человека (например, ложный запуск программы, нечаянно допущенные из-за несоблюдения правил безопасности работы в Интернете инсталляции закладок и т.п.); умышленные (инспирированы), результат умышленных действий людей (например, умышленная установка программ, которые передают информацию на другие компьютеры, преднамеренное заражение вирусами, нарочитая дезинформация и т.п.).

По степени гипотетической вреда:

• ***угроза*** - явные или потенциальные действия, которые затрудняют или делают невозможным реализацию национальных интересов в информационной сфере и создают опасность для системы управления национальной безопасностью, жизнеобеспечение ее системообразующих элементов;

• ***опасность*** - непосредственная дестабилизация функционирования системы управления национальной безопасностью.

По повторяемостью совершения:

• ***повторяющиеся*** - такие угрозы, которые имели место ранее;

• ***продолжающиеся*** - неоднократное осуществление угроз, состоящий из ряда тождественных угроз, которые имеют общую цель.

По сферам происхождения:

• ***экзогенные*** - источник дестабилизации системы лежит за ее пределами;

• ***эндогенные*** - алгоритм дестабилизации системы находится в самой системе.

По вероятности реализации:

• ***вероятные***;

• ***невозможные*** - угрозы обычно имеют более декларативный характер, не подкрепленный реальной и даже потенциальной возможностью осуществить провозглашенные намерения, они в основном имеют запугивающий характер;

• ***случайные*** - угрозы, за выполнение определенного комплекса условий каждый раз протекает по-разному. Угрозы данного уровня целесообразно анализировать с помощью методов исследования операций, в частности теории вероятностей и теории игр, которые изучают закономерности в случайных явлениях.

По уровню детерминизма:

• ***закономерные*** - такие угрозы, которые носят устойчивый, повторяющийся характер, обусловленные объективными условиями существования и развития системы информационной безопасности. Так, например, любой субъект системы обеспечения национальной безопасности подвергаться информационным атакам, если в нем не работает, или работает не на должном уровне система обеспечения ИБ.

• ***случайные*** - угрозы, которые могут или случиться либо не случиться.

По значению:

• ***допустимые*** - такие угрозы, которые не могут привести к коллапсу системы. Примером могут служить вирусы, не повреждают программы путем их уничтожения;

• ***недопустимые*** - такие угрозы, которые: 1) могут в случае их реализации привести к коллапсу и системной дестабилизации системы; 2) могут привести к изменениям, не совместимых с дальнейшим существованием СНБ.

По структуре воздействия:

• ***системные*** - угрозы, влияющие сразу на все составляющие элементы системы управления национальной безопасностью;

• ***структурные*** - угрозы, влияющие на отдельные структуры системы;

• ***элементные*** - угрозы, влияющие на отдельные элементы структуры системы.

По характеру реализации: ***реальные, потенциальные,***

По объекту воздействия: лицо; общество; государство**.**

РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ПРАКТИЧЕСКИМ (СЕМИНАРСКИМ) ЗАНЯТИЯМ И ВЫПОЛНЕНИЕ СРС

Студентам следует:

- до очередного семинарского занятия по рекомендованным литературным источникам проработать теоретический материал, соответствующей темы занятия;
- при подготовке к семинарским занятиям следует обязательно использовать не только лекции, учебную литературу, но и нормативно-правовые акты, интернет-источники и информационные ресурсы информационно-образовательного портала Финансового университета;
- в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении, при решении задач, заданных для самостоятельного решения и вопросов;
- в ходе семинара давать конкретные, четкие ответы по существу вопросов;
- на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

Студенты, не отчитавшиеся по каждой не проработанной ими на занятиях теме к началу зачетной сессии, упускают возможность получить положенные баллы за работу в семестре.

Методические рекомендации по выполнению различных форм самостоятельных домашних заданий. Самостоятельная работа – учебная, научно-исследовательская работа студентов, выполняемая во внеаудиторное время по заданию и под руководством преподавателя. Самостоятельная работа предполагает усвоение теоретического материала на базе изучения и систематизации материалов первоисточников, монографий, статей и т.п. Преподаватель планирует содержание и объем самостоятельной работы, контролирует результаты самостоятельной работы. Самостоятельная работа включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемой дисциплины. По каждой теме учебной дисциплины предлагается перечень заданий/вопросов для самостоятельной работы.

В процессе освоения дисциплины студенты выполняют контрольную работу, предусмотренную учебным планом.

Для подготовки к семинарским (практическим) занятиям обучающимся необходимо изучить материалы по дисциплине, представленные на ИОП Финуниверситета, литературные и интернет-источники, рекомендованные преподавателем, ответить на вопросы изучаемой темы.

Вопросы для самоподготовки к семинарским занятиям

Тема 1. Информационная безопасность в системе национальной безопасности

1. Что такое информационная безопасность?
2. Виды национальной безопасности. Приведите характеристику каждого вида.
3. Какие существуют системные связи информационной безопасности с другими видами национальной безопасности? Приведите примеры.

Тема 2. Правовое и организационное обеспечение информационной безопасности

1. Перечислите задачи государства в области безопасности информации.
2. Раскройте основные положения Доктрины информационной безопасности Российской Федерации.

3. Охарактеризуйте основные законы РФ, регулирующие отношения в области информационных технологий и информационной безопасности.

4. Назовите государственные органы, обеспечивающие безопасность информационных технологий, и решаемые ими задачи.

5. Дайте общую характеристику организационным методам защиты информации в ИС.

Тема 3. Основы управления информационными рисками

1. Чем обусловлена необходимость перехода от управления информационной безопасностью к управлению информационными рисками?

2. Дайте определение информационного риска в узком и расширенном смыслах.

3. Как соотносятся между собой понятия «информационный риск» и «экономическая безопасность предприятия»?

4. Приведите принципы управления информационными рисками.

5. Перечислите задачи управления информационными рисками и раскройте их содержание.

6. Каковы возможные стратегии управления информационными рисками?

Тема 4. Информационные уязвимости объектов

1. Что такое антропогенные информационные уязвимости?

2. Что такое техногенные информационные уязвимости?

3. Приведите классификацию информационных уязвимостей.

Тема 5. Угрозы информационной безопасности и их источники

1. Приведите определения эндогенных, экзогенных, антропогенных и техногенных угроз информационной безопасности.

2. Приведите классификацию техногенных угроз информационной безопасности.

3. Что такое угрозы конфиденциальности, целостности и доступности информации?

4. Раскройте понятие «Информационная война» и приведите примеры.

Тема 6. Методы и средства обеспечения информационной безопасности компьютерных систем

1. Что такое стеганография?

2. Что такое криптография?

3. Что называется криптосистемой?

4. Что такое криптоанализ?

5. Приведите классификацию методов шифрования.

6. Перечислите требования, которым должны отвечать современные методы шифрования.

7. Приведите процедуру использования открытого ключа.

8. Приведите алгоритм зашифрования с помощью таблицы Виженера.

9. Приведите алгоритм расшифрования с помощью таблицы (матрицы) Виженера.

10. В чем заключается различие блочных и поточных шифров?

11. Что устанавливает электронная подпись?

Тема 7. Риски информационной безопасности и проблема построения комплексной системы защиты информации

1. Раскройте алгоритм управления информационными рисками.

2. Определите понятие «система управления информационными рисками» и раскройте научные принципы ее построения.

3. Перечислите задачи, решаемые в процессе создания системы управления

информационными рисками.

Тема 8. Особенности защиты информации в распределенных компьютерных системах

1. Поясните принципы защиты речевой информации в каналах связи.
2. Перечислите и охарактеризуйте методы защиты от прослушивания акустических сигналов.
3. Охарактеризуйте средства борьбы с закладными подслушивающими устройствами.

Тема 9. Обработка и передача информации в компьютерных и управляющих системах и сетях связи, вопросы информационной безопасности и защиты информации для компьютерных и управляющих систем и сетей

1. В чем заключается сущность матричного (дискреционного) метода доступа?
2. Сравните матричный и мандатный методы доступа.
3. Перечислите основные способы неявного задания матрицы доступа и охарактеризуйте их.
4. Какие элементы содержит система разграничения доступом и как они взаимодействуют в процессе обслуживания запроса на доступ к объекту?
5. Приведите основные возможности ОС Windows по разграничению доступа.
6. Какими возможностями по разграничению доступа обладают приложения MS Office?
7. Назовите основные принципы разработки алгоритмов, программ и технических средств.
8. В чем заключается суть современных технологий программирования?
9. Дайте характеристику автоматизированной системы разработки программных средств.
10. Каким образом достигается защита от несанкционированного изменения структур КС на этапах разработки и эксплуатации?
11. Как осуществляется контроль целостности информации?
12. Как работает алгоритм защиты информации по протоколу Керберос?

Тема 10. Защита компьютерных систем от вирусов и вредоносных программ

1. Перечислите этапы жизненного цикла компьютерного вируса.
2. Приведите классификацию компьютерных вирусов.
3. Дайте характеристику загрузочным вирусам.
4. Дайте характеристику вирусам-мутантам.
5. Дайте характеристику макрокомандным вирусам.
6. Дайте характеристику программе-вирусу.
7. Дайте характеристику вирусу «троянский конь».
8. Дайте характеристику вирусу «червь».
9. Дайте характеристику антивирусным программам.
10. Перечислите рекомендации по антивирусной защите.
11. Какие компоненты входят в межсетевые экраны?
12. Перечислите основные функции межсетевого экрана (firewall).
13. Перечислите симптомы заражения компьютера вирусом.

Темы докладов/ рефератов

1. Основные понятия и составляющие информационной безопасности
2. Доктрина информационной безопасности Российской Федерации и ее основные положения

3. Классификация угроз информационной безопасности. Наиболее распространенные угрозы информационной безопасности
4. Классификация компьютерных вирусов и вредоносных программ
5. Источники проникновения вирусов и средства защиты от вирусов и вредоносных программ
6. Комплексный подход к задаче защиты от вирусов и вредоносных программ в компьютерной системе
7. Защита компьютерных систем от электромагнитных излучений и наводок. Активные и пассивные методы
8. Симметричные, асимметричные и гибридные криптоалгоритмы и их использование на современном этапе
9. Автоматизированные системы шифрования и области их применения
10. Основные понятия политики информационной безопасности предприятия
11. Основные понятия информационной защиты сетей
12. Средства информационной защиты сетей и защита по протоколу Керберос
13. Виды стандартов информационной безопасности
14. Стандарт «Оранжевая книга» (понятие «доверенная система»; определение «Уровня гарантированности»; политика безопасности и ее элементы)
15. Отличия алгоритмов DES и ГОСТ 28147-89
16. Уголовный кодекс Российской Федерации: преступления в сфере компьютерной информации
17. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации в ФЗ «Об информации, информационных технологиях и защите информации»
18. Методы и средства обеспечения безопасной работы в глобальной сети Интернет
19. Обеспечение информационной безопасности процессов функционирования систем электронной торговли
20. Обеспечение информационной безопасности процессов функционирования систем дистанционного банковского обслуживания
21. Защита информации в каналах связи
22. Применение методов криптографии для идентификации и аутентификации удаленных процессов
23. Межсетевое экранирование и его использование для защиты информации в распределенных компьютерных системах
24. Средства операционных систем и Microsoft Office по защите от несанкционированного доступа к документам
25. Методы контроля целостности информации. Защита от НСД к внутреннему монтажу, средствам коммутации, от подключения нештатных устройств

Задания

1. Были ли в вашей практике случаи попыток несанкционированного получения информации, обрабатываемой в АС? Охарактеризуйте проявившийся в каждом конкретном случае канал несанкционированного доступа и оцените возможную уязвимость информации.
2. Какие вам известны подходы к классификации угроз безопасности информации? Сравните их между собой с точки зрения наибольшего соответствия практическим потребностям создания систем защиты информации.
3. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.

4. Рассмотрите возможности несанкционированного получения информации в следующем случае:

- в рассматриваемой АС возможны нарушители двух категорий: внешние, не имеющие отношения к системе, и внутренние, входящие в состав персонала, обслуживающего АС;

- объектами несанкционированных действий, являются магнитные носители информации, видеотерминалы ввода-вывода информации и принтеры;

- каналами несанкционированного получения информации являются непосредственное хищение носителей, просмотр информации на экране дисплея и выдача ее на печать.

Каковы, с вашей точки зрения, в этом случае вероятности несанкционированного получения информации?

5. В чем, с вашей точки зрения, состоит опасность разработки и применения информационного оружия? Какие необходимо было бы применить меры международного характера в целях предотвращения информационных войн?

6. Каковы основные принципы защиты информации от несанкционированного доступа? В чем заключается суть каждого из них?

7. Представьте следующую ситуацию: министры внутренних дел и экономики имеют одинаковую (наивысшую) форму допуска и пытаются с помощью автоматизированной системы получить строго конфиденциальную информацию по вопросу расследования экономических преступлений. Каковы, на ваш взгляд, должны быть возможности их доступа к этой информации? Рассмотрите все возможные ситуации и последствия, к которым приведут принимаемые решения по доступу с точки зрения обеспечения безопасности информации.

8. Сравните различные известные вам модели защиты от несанкционированного доступа к информации.

9. Что можно сказать о взаимодействии уровней безопасности субъектов и объектов доступа для различных видов доступа, с которыми оперирует модель Белла – Ла Падула?

10. Дайте определения идентификации и аутентификации пользователей. В чем разница между этими понятиями?

11. Назовите основные способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным?

12. Приведите примеры известных вам систем аутентификации, построенных по принципу «пользователь имеет». Что вы можете сказать о преимуществах и недостатках методов аутентификации пользователей пластиковых карт, широко используемых в банковской сфере?

13. Каковы основные характеристики устройств аутентификации? Сравните известные вам устройства по каждой из этих характеристик.

14. Какие основные методы контроля доступа используются в современных автоматизированных системах? Охарактеризуйте эти методы и рассмотрите их возможности для реализации автоматизированной системы ведения текущих счетов клиентов банка.

15. Охарактеризуйте процесс развития проблемы защиты информации в современных системах ее обработки.

16. Раскройте содержание разграничения доступа к информации с помощью монитора обращений.

17. Охарактеризуйте проблему определения предметной области информационной безопасности и дайте определения основным понятиям, используемым в этой сфере.

18. Раскройте содержание исторических этапов развития подходов к защите информации и обеспечению информационной безопасности.

19. Охарактеризуйте «вредительские» программы как один из видов угроз информационной безопасности.

20. Раскройте содержание модели разграничения доступа Лэмпсона – Грэхема – Деннинга.

21. Раскройте содержание принципов обоснованности доступа и персональной ответственности как основных принципов защиты от несанкционированного доступа.

22. В чем состоит суть принципов достаточной глубины контроля и разграничения потоков информации как основных принципов защиты информации от несанкционированного доступа?

23. Раскройте содержание принципов чистоты повторно используемых ресурсов и целостности средств защиты как основных принципов защиты информации от несанкционированного доступа.

24. Раскройте основные особенности известных вам методов аутентификации с использованием индивидуальных физиологических характеристик пользователей.

25. Рассмотрите основные методы повышения стойкости парольных систем аутентификации пользователей автоматизированных систем.

26. Что изучают криптография, криптоанализ и криптология? Дайте определения этим наукам.

27. Какие методы криптографического закрытия информации вы знаете? В чем разница между шифрованием и кодированием?

28. Объясните, что представляет собой стеганография?

29. Расскажите об особенностях симметричных и несимметричных шифров. Попробуйте привести примеры этих способов шифрования.

30. Объясните, почему основными требованиями, предъявляемыми к криптосистемам, являются наличие очень большого числа возможных ключей и равная вероятность их генерации.

31. От каких основных свойств криптографических алгоритмов зависит, на ваш взгляд, стойкость криптосистемы?

32. В чем принципиальное различие оценки стойкости криптосистемы с использованием теории информации и теории вычислительной сложности?

33. Какие основные способы шифрования вы знаете? Каковы их преимущества и недостатки?

34. Опишите наиболее известный алгоритм шифрования DES. Какие из основных методов шифрования использованы в этом алгоритме?

35. Каковы основные особенности криптосистем с общедоступным ключом?

36. Раскройте основное содержание алгоритма электронной подписи.

37. Какие методы распределения ключей в криптографических системах с большим числом абонентов вы знаете? Охарактеризуйте основные особенности децентрализованных и централизованных систем.

38. Опишите последовательность установления связи и передачи сообщений в централизованных системах распределения ключей шифрования с центром трансляции ключей и с центром распределения ключей.

39. В каких случаях применяются криптографические методы защиты информации непосредственно в ЭВМ?

40. Дайте определение компьютерного вируса как саморепродуцирующейся программы. Приведите примеры известных вам случаев заражения компьютеров вирусами.

41. Попробуйте изобразить структуру компьютерного вируса в виде программы, написанной на псевдоязыке.

42. Охарактеризуйте основные фазы, в которых может существовать компьютерный вирус.

43. Охарактеризуйте известные вам основные классы антивирусных программ. В чем смысл комплексного применения нескольких программ?

44. Каковы, на ваш взгляд, должны быть основные правила работы с компьютером, предупреждающие возможное заражение его вирусами?

45. Охарактеризуйте перспективные методы защиты компьютеров от программ-вирусов.

46. Рассмотрите возможности вирусного подавления как одной из форм радиоэлектронной борьбы.

47. Каковы основные механизмы внедрения компьютерных вирусов в поражаемую систему?

48. Раскройте содержание комплексной стратегии защиты, ориентированной на противодействие возможному вирусному подавлению.

49. Дайте определение понятию «технический канал утечки информации». Назовите основные виды технических каналов.

50. Какой, по вашему мнению, технический канал утечки информации можно отнести к наиболее часто используемым техническими разведками для получения конфиденциальной информации? Раскройте особенности этого канала.

51. Дайте классификацию источников утечки информации по техническим каналам.

52. Что такое основные и вспомогательные технические средства автоматизированной системы? Приведите примеры и рассмотрите возможности их использования в качестве технических каналов утечки информации.

53. Назовите известные вам методы и средства контроля акустической информации.

54. Охарактеризуйте методы контроля информации техническими средствами в каналах телефонной связи.

55. Назовите методы контроля информации, обрабатываемой средствами вычислительной техники.

56. Охарактеризуйте основные способы предотвращения утечки информации по техническим каналам.

57. Приведите известные вам методы защиты от утечки информации по акустическому каналу. Попробуйте сравнить их, используя критерий «эффективность/стоимость».

58. Охарактеризуйте существующие на сегодняшний день способы защиты информации в каналах связи.

59. Назовите методы и средства защиты информации от утечки по побочному электромагнитному каналу.

60. С чем, по вашему мнению, связана необходимость организационно-правового обеспечения защиты информации? в чем заключается специфика этого обеспечения применительно к информации, обрабатываемой в автоматизированных системах?

61. Охарактеризуйте задачи, решаемые организационно-правовым обеспечением защиты информации в АС. Выделите особенности, связанные с «электронной» формой представления информации в АС.

62. Сформулируйте основные направления развития организационно-правового обеспечения защиты информации в зарубежных странах. Назовите известные вам законодательные акты зарубежных стран в области регулирования процессов информатизации и обеспечения безопасности информации.

63. Что вы знаете из истории развития организационно-правового обеспечения зашиты информации в СССР и Российской Федерации? Охарактеризуйте современное состояние отечественной законодательной базы в области информатизации и защиты информации.

64. Сформулируйте основные положения Закона Российской Федерации «Об информации, информационных технологиях и защите информации». Какие еще вы знаете российские законодательные акты в этой области?

65. Сформулируйте основные подходы к разработке организационно-правового обеспечения защиты информации. Раскройте содержание структуры этого обеспечения.

66. Сформулируйте основные требования, предъявляемые к системе стандартизации в области защиты информации. Назовите известные вам системы стандартов в этой области, принятые в России и за рубежом.

67. Опишите систему органов государственного управления Российской Федерации, осуществляющих управление и координацию деятельности в области защиты информации и обеспечения информационной безопасности.

68. Изложите кратко основное содержание деятельности ФСТЭК России в области обеспечения информационной безопасности.

69. Почему, на ваш взгляд, действительно эффективная защита информации может быть обеспечена только при комплексном системном подходе к решению этой проблемы? В чем заключается комплексность? Каким требованиям должна удовлетворять концепция комплексной защиты?

70. Сформулируйте основные концептуальные положения теории защиты информации.

71. Раскройте содержание функции защиты информации. Какие из функций образуют полное множество функций защиты?

72. Сформулируйте определение задачи защиты информации и попытайтесь назвать десять классов задач, образующих репрезентативное множество задач защиты.

73. Приведите наиболее распространенную на сегодняшний день классификацию средств защиты информации. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств защиты информации?

74. Дайте определение системы защиты информации и сформулируйте основные концептуальные требования, предъявляемые к ней.

75. Раскройте содержание концепции управления системой защиты информации. Каковы ее особенности по сравнению с общей концепцией управления системами организационно-технологического типа?

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ КОНТРОЛЬНОЙ РАБОТЫ

1. Цель организации выполнения контрольной работы и ее структура

В соответствии с учебным планом в процессе изучения дисциплины «Информационная безопасность компьютерных систем» студенты, обучающиеся по направлению 380305 «Бизнес-информатика», квалификация (степень) бакалавр, выполняют контрольную работу.

Целью контрольной работы является углубленное изучение вопросов, касающихся теоретических основ информационной безопасности, классификации угроз информационной безопасности, стандартов и современных технологий обеспечения информационной безопасности, а также приобретение навыков в шифровании исходной информации и работы в среде систем обеспечения информационной безопасности.

Студент должен изучить рекомендуемую учебную литературу и ознакомится с методическими указаниями по выполнению контрольной работы.

Контрольная работа состоит из двух заданий. Задание 1 представляет собой теоретический вопрос, для раскрытия которого студенту рекомендуется подобрать и изучить литературу, изданную не ранее последних пяти лет от года написания

контрольной работы. Это могут быть учебные пособия и учебники, рекомендованные по направлению подготовки бакалавров в высшей школе, а также монографии, статьи из журналов и др.

Практическая часть контрольной работы представлена заданием 2.

Каждое задание должно быть выполнено по вариантам в соответствии со следующей структурой:

- номер варианта задания и тема задания;
- условие задания;
- материал, раскрывающий тему задания/ или описание алгоритмов решения задач, приведенных в задании 2.

Структура контрольной работы следующая:

Титульный лист
Содержание
Введение
1. Теоретическая часть
< Задание 1 >
Заключение
2. Практическая часть
< Задание 2 >
2.1. Условие задания 2
2.2. Алгоритм решения задания 2
Список использованной литературы
Приложения

Титульный лист является первой страницей контрольной работы, однако он не нумеруется. Образец титульного листа контрольной работы приведен в Приложении 1.

В ***содержании*** необходимо привести все заголовки структурных частей работы с указанием страниц, с которых они начинаются. Исключение сделано для подзаголовков, даваемых в подбор с текстом. Заголовки должны соответствовать заголовкам теоретической части, т.е. заголовкам параграфов. Последнее слово каждого заголовка соединяется отточием с соответствующим ему номером страницы в правом столбце содержания.

Во ***введении*** студент должен обосновать актуальность раскрываемой темы, указать цель, объект изучения и перечень вопросов (задач), которые будут рассмотрены в *теоретической части*.

План изложения *теоретической части* должен быть продуман и выполнен студентом после проработки литературных и электронных источников. При составлении плана теоретической части необходимо учесть и рассмотреть следующее:

- *понятия*, используемые при изучении объекта или процесса, т.е. перечислить основные понятия, используемые в выбранной теме;
- *содержание теоретической части*, с использованием введенных понятий, схем, рисунков, таблиц, диаграмм и т.д. и изложением не только собственных умозаключений, но и мнений различных авторов по данной теме, с обязательным указанием ссылок на литературные источники.

Теоретическая часть может состоять из двух, трех или более параграфов. Однако делать параграфы слишком маленькими по объему не следует. Здесь студент демонстрирует свое умение подбирать материал по теме из печатных и электронных источников и четкость структуры теоретической части. Заголовки параграфов дают однозначное понимание раскрываемой тематики.

Заключение – не более 2 страниц. Оно не должно слово в слово повторять уже имеющийся текст, а должно содержать собственные *выводы* студента, полученные в

результате проведенной работы, и может содержать материал о *перспективах* развития исследуемой темы.

Литературные источники – это учебники и учебные пособия, рекомендованные для студентов высших учебных заведений, журналы, электронные издания и др., указанные в списке использованной литературы, оформленные в соответствии с правилами и относящиеся к последним пяти годам. (Исключение составляют ГОСТ, ГОСТ ИСО/МЭК, ФЗ и др. нормативные документы.)

В ***списке литературы*** студент приводит литературу, использованную им в процессе написания контрольной работы. В список должны включаться только те источники, на которые имеются ссылки, приведенные в теоретической части работы.

Образцы корректного оформления литературы приведены ниже:

1) *ГОСТы, учебники, учебные пособия, методические указания и т.д.*

1. ГОСТ 17799-2005 (ISO 17799:2005). Практические правила управления информационной безопасностью.

2. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2016.

4. Завгородний В.И. Учебное пособие по дисциплине «Информационная безопасность», М.: Финуниверситет, 2016.

2). *Электронные ресурсы*

1. Гухман В.Б., Тюрина Е.И. Основы защиты данных в Microsoft Office [Электронный ресурс] // Официальный сайт интернет университета информационных (www.intuit.ru). 23.05.2016. URL: http://www.intuit.ru/department/se/intuml.

В ***приложениях*** приводят материалы, которые дополняют теоретическую часть работы. По форме данные материалы могут быть представлены в виде текста, таблиц, рисунков, схем, графиков и диаграмм. Каждое приложение должно начинаться с новой страницы с указанием в правом верхнем углу слова «Приложение» и номера, а также должно иметь тематический заголовок. При наличии в работе более одного приложения необходимо нумеровать их арабскими цифрами. Например:

Приложение 5
Характеристика средств защиты от электромагнитных излучений
< Материалы приложения >
. . . . . .

Связь основного текста с приложениями осуществляется через ссылки.

2. Требования к оформлению контрольной работы

Контрольная работа оформляется на ПК с использованием текстового процессора Microsoft Word на листах формата А4, ориентация – книжная.

Следует установить следующие размеры полей страницы: левое поле – 3 см, правое, верхнее и нижнее – 2 см.

Требования к оформлению текста контрольной работы:

– отступ первой строки (абзацный отступ) – 1,25 см;

– междустрочный интервал – 1,5 строки;

– гарнитура шрифта – Times New Roman;

– кегль шрифта (размер) – 14 пунктов;

– форматирование текста (выравнивание) – по ширине.

Каждую структурную часть контрольной работы нужно начинать с нового листа. Точка в конце заголовка структурной части работы не ставится.

Каждая цитата, заимствованные цифры, факты должны сопровождаться ссылкой на источник, описание которого приводится в списке использованной литературы. В ссылке указывается номер источника по списку и номера страниц, например: [7, С.45-46].

Все аббревиатуры и сокращения слов должны быть расшифрованы в тексте работы при первом употреблении.

Математические формулы оформляются с помощью редактора формул – приложения EQNEDT32.exe.

Рисунки необходимо снабжать подрисуночной подписью, например:

< Рисунок >

. . . . . .

Рис. 3. Взаимосвязь между методами и средствами защиты информации

В конце подрисуночной подписи точку не ставят.

Все схемы и рисунки имеют одинарную сквозную нумерацию. Нельзя располагать подрисуночную подпись и рисунок на разных страницах. На все рисунки необходимо сделать ссылки в тексте контрольной работы.

Табличный материал (таблица) оформляется следующим образом. В правом верхнем углу пишут слово «Таблица» и ее порядковый номер в работе. Таблица должна иметь тематический заголовок, который располагают по центру без точки в конце, например:

Таблица 3

Таблица Виженера

< Таблица >

. . . . . .

Допускается использование в таблице кегля шрифта (размера) – 12 пунктов.

На последней странице контрольной работы студент обязан поставить дату сдачи контрольной работы на регистрацию и свою подпись.

Контрольная работа должна быть сброшюрована по левому краю.

Образец титульного листа контрольной работы приведен в Приложении 1 данного раздела.

Объем контрольной работы не более 15 страниц, включая титульный лист и список литературы. Приложения, если они есть, в общем объеме контрольной работы не учитываются.

3. Задания контрольной работы

Задание 1

3.1. Цель выполнения задания 1

3.1.1. Изучение методов и средств комплексной защиты информации в информационных системах предприятий и организаций.

3.1.2. Формирование навыков анализа защищенности информационных систем, использования встроенных возможностей операционных систем, Microsoft Office, брандмауэров, антивирусных и криптографических методов и средств для обеспечения безопасности информации.

3.2. Содержание и варианты задания 1

3.2.1. Предлагается следующий план раскрытия темы задания 1:

Введение (объем – 1 страница)

1. Теоретическая часть на тему «Тема задания 1» (объем – 8-10 страниц)

1.1. ….....

1.2. ….....

1.3. ….....

Заключение (объем – 1-2 страницы)

3.2.2. Варианты задания 1 приведены в табл. 1. Номер варианта выполнения задания 1 соответствует порядковому номеру студента в списке журнала группы.

Таблица 1. **Варианты задания 1**

Номер варианта	**Тема задания 1**
1	2
1	Основные понятия и составляющие информационной безопасности
2	Доктрина информационной безопасности Российской Федерации и ее основные положения
3	Классификация угроз информационной безопасности. Наиболее распространенные угрозы информационной безопасности
4	Классификация компьютерных вирусов и вредоносных программ
5	Источники проникновения вирусов и средства защиты от вирусов и вредоносных программ
6	Комплексный подход к задаче защиты от вирусов и вредоносных программ в компьютерной системе
7	Защита компьютерных систем от электромагнитных излучений и наводок. Активные и пассивные методы
8	Симметричные, асимметричные и гибридные криптоалгоритмы и их использование на современном этапе
9	Автоматизированные системы шифрования и области их применения
10	Основные понятия политики информационной безопасности предприятия
11	Основные понятия информационной защиты сетей
12	Средства информационной защиты сетей и защита по протоколу Керберос
13	Виды стандартов информационной безопасности
14	Стандарт «Оранжевая книга» (понятие «доверенная система»; определение «Уровня гарантированности»; политика безопасности и ее элементы)
15	Отличия алгоритмов DES и ГОСТ 28147-89
16	Уголовный кодекс Российской Федерации: преступления в сфере компьютерной информации
17	Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации в ФЗ «Об информации, информационных технологиях и защите информации»
18	Методы и средства обеспечения безопасной работы в глобальной сети Интернет
19	Обеспечение информационной безопасности процессов функционирования систем электронной торговли
20	Обеспечение информационной безопасности процессов функционирования систем дистанционного банковского обслуживания
21	Защита информации в каналах связи
22	Применение методов криптографии для идентификации и аутентификации удаленных процессов
23	Межсетевое экранирование и его использование для защиты информации в распределенных компьютерных системах

24	Средства операционных систем и Microsoft Office по защите от несанкционированного доступа к документам
25	Методы контроля целостности информации. Защита от НСД к внутреннему монтажу, средствам коммутации, от подключения нештатных устройств

Задание 2

3.3. Цель выполнения задания 2

3.3.1. Изучение методики полиалфавитной замены с использованием таблицы (матрицы) Виженера.

3.3.2. Приобретение практических навыков в зашифровании исходного текста и расшифровании шифртекста (криптограммы).

3.4. Содержание и варианты задания 2

3.4.1. Изучение методики зашифрования с помощью таблицы (матрицы) Виженера. Методика зашифрования исходного текста приведена в п. 3.5.

3.4.2. Изучение методики расшифрования с помощью таблицы (матрицы) Виженера. Методика расшифрования криптограммы приведена в п. 3.5.

3.4.3. Используя таблицу Виженера, приведенную в Приложении 2, решить задачи зашифрования исходного текста и расшифрования шифртекста. Исходные данные для решения задач приведены в табл. 2. Номер варианта выполнения задания 2 соответствует порядковому номеру студента в списке журнала группы.

Таблица 2. Варианты задания 2

Номер варианта	Исходный текст	Ключ зашифрования	Шифртекст (криптограмма)	Ключ расшифрования
1	2	3	4	5
1	Система защиты информации	шифр	ЙБНСНЕЭЛЮНМЧЗ	шпион
2	Метод высокочастотного навязывания	ключ	ЧЮШЫТЫОЭМЛХХ	норма
3	Симметричные и асимметричные шифры	вирус	ДНЖАЪЗТЭФК	метр
4	Источник, фактор и причина риска	метод	ГИЫХВРКШЧ	лазер
5	Информационная безопасность	бит	ЛЭЗЩДЙУИ	луч
6	Информационный риск	знак	ЖЮХЧЮНАЪН	фон
7	Конфиденциальность информации	блок	ЙКЧПХТУСЙЗЧФЗ	звук
8	Внешние и внутренние угрозы	язык	ЪКТДГЩЩМВЕБДХ	цель
9	Каналы утечки звуковой информации	гост	ББТСЯИОУЬБТУС	сбой
10	Источник информационного риска	схема	ЮЙФЙИНГДАЕЕДХ	цепь
11	Уязвимость компью-	шаг	УЛЫЛЗОРО	люк

	терной системы			
12	Система управления информационными рисками	буква	СЙЮДЮНГОБЕДКБ	сеть
13	Анализ информа-ционных рисков	червь	ЬЪЦЫПИЖА	лицо
14	Методы традиционного шпионажа и диверсий	строка	РЖЬЕЭЕТФШЭКЦШТ	рука
15	Случайные и предна-меренные угрозы	число	ЗЮБТЛЫОЙГШИМ	глаз
16	Несанкционированная модификация прог-раммной структуры информационной системы	акростих	ЯРПШЧХАГЧК	план
17	Несанкционирован-ный доступ к информации	пульт	ЭЯШЭИЫП	эхо
18	Стандарты управления системами информационной безопасности	алгоритм	НЮМЬУЮКФРШН	гриф
19	Организационные методы защиты информации	скрытие	СРЕЖШХЕЮЪЕ	речь
20	Надежность и отказоустойчивость информационных систем	риск	БРХЩРУЪУРЮЪЛ	ритм
21	Помехоустойчивое кодирование информации	закон	ЭГТБЧЙЬЬОЯГШ	ухо
22	Методы биометрической идентификации человека	угроза	ВМЮЙЭГЩМБРРДЮКУ	свод
23	Абсолютно надежный шифр	код	ЫЧРПМРАПЮМ	урок
24	Дискреционный и мандатный методы доступа	сбор	ЭГРАТЩЯРЙКВЮХ	среда
25	Система разграничения доступа к информации	сигнал	ИЗЧХЖЦРХФЮМИКЭДГ	дверь

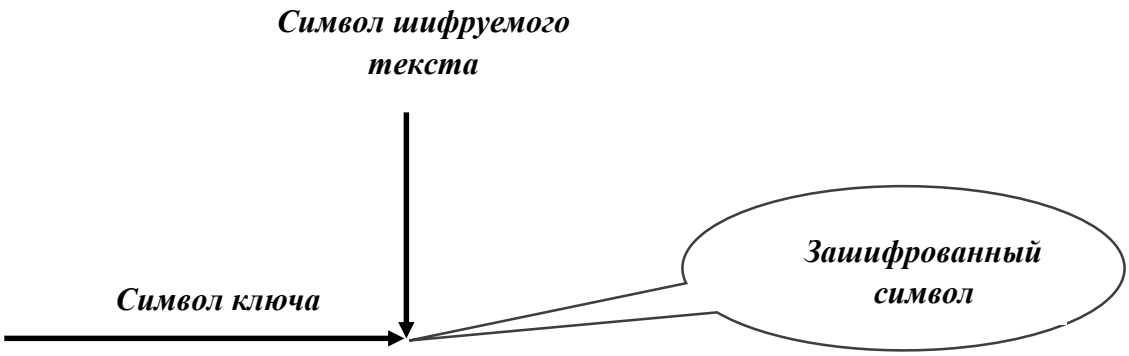
3.5. Методика и примеры выполнения задания 2

3.5.1. Процесс ***зашифрования*** исходного текста состоит в следующем:

а) под каждым символом шифруемого исходного текста записываются символы ключа, повторяющие ключ требуемое число раз;

б) символ шифруемого текста определяет столбец таблицы, а символ ключа – ее строку. Зашифрованный символ находится на пересечении строки и столбца.

Схематично данную операцию можно представить следующим образом:



Пример зашифрования исходного текста. С помощью ключа ЗАРЯ создайте криптограмму (шифртекст) для слова СЧЕТ.

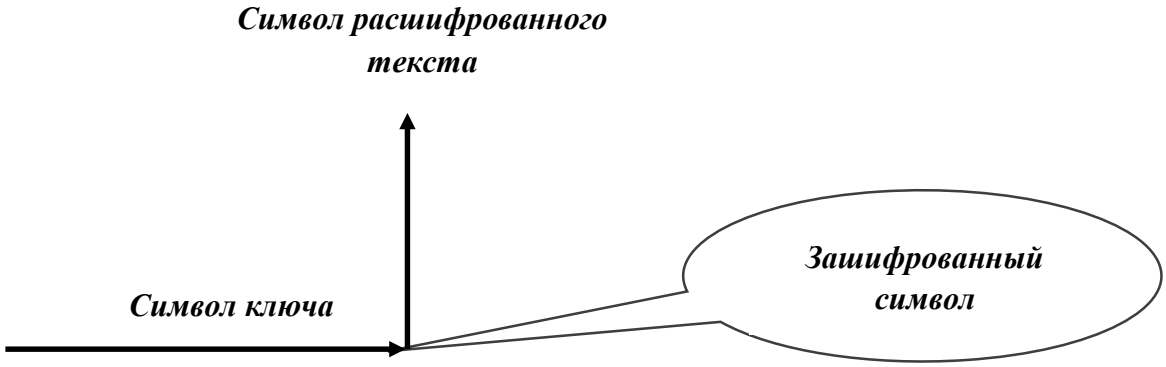
Исходный текст: **СЧЕТ**
Ключ: **ЗАРЯ**
Шифртекст: **ШЧХС**

3.5.2. Процесс ***расшифрования*** предполагает выполнение обратной процедуры:

а) над символами зашифрованного текста сверху последовательно записываются символы ключа;

б) символ ключа определяет строку таблицы, а символ зашифрованного текста – ее столбец. Символ, находящийся в первой строке таблицы, является символом расшифрованного текста.

Схематично данную операцию можно представить следующим образом:



Пример расшифрования исходного текста. С помощью ключа ЧЕК расшифруйте криптограмму (шифртекст) **ИПХЧЙ**.

Ключ: **ЧЕКЧЕ**
Шифртекст: **ИПХЧЙ**
Исходный текст: **СКЛАД**

ПРИЛОЖЕНИЕ 1

Образец титульного листа контрольной работы

Федеральное государственное образовательное бюджетное учреждение
высшего образования
«Финансовый университет при Правительстве Российской Федерации»

Новороссийский филиал

Кафедра «Информатика, математика и общегуманитарные науки»

Контрольная работа

по дисциплине **«Информационная безопасность»**

Исполнитель: студент
<Фамилия И.О.>
направление:
бакалавр бизнес-информатики
группа: 1б-ббби100
номер зачетной книжки:
11флб00838
Руководитель:
<уч. степень, должность Фамилия И.О.>

Новороссийск 201_

Таблица Виженера

*	АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
А	абвгдежзийклмнопрстуфхцчшщъыьэюя
Б	бвгдежзийклмнопрстуфхцчшщъыьэюяА
В	вгдежзийклмнопрстуфхцчшщъыьэюяАБ
Г	гдежзийклмнопрстуфхцчшщъыьэюяАБВ
Д	дежзийклмнопрстуфхцчшщъыьэюяАБВГ
Е	ежзийклмнопрстуфхцчшщъыьэюяАБВГД
Ж	жзийклмнопрстуфхцчшщъыьэюяАБВГДЕ
З	зийклмнопрстуфхцчшщъыьэюяАБВГДЕЖ
И	ийклмнопрстуфхцчшщъыьэюяАБВГДЕЖЗ
Й	йклмнопрстуфхцчшщъыьэюяАБВГДЕЖЗИ
К	клмнопрстуфхцчшщъыьэюяАБВГДЕЖЗИЙ
Л	лмнопрстуфхцчшщъыьэюяАБВГДЕЖЗИЙК
М	мнопрстуфхцчшщъыьэюяАБВГДЕЖЗИЙКЛ
Н	нопрстуфхцчшщъыьэюяАБВГДЕЖЗИЙКЛМ
О	опрстуфхцчшщъыьэюяАБВГДЕЖЗИЙКЛМН
П	прстуфхцчшщъыьэюяАБВГДЕЖЗИЙКЛМНО
Р	рстуфхцчшщъыьэюяАБВГДЕЖЗИЙКЛМНОП
С	стуфхцчшщъыьэюяАБВГДЕЖЗИЙКЛМНОПР
Т	туфхцчшщъыьэюяАБВГДЕЖЗИЙКЛМНОПРС
У	уфхцчшщъыьэюяАБВГДЕЖЗИЙКЛМНОПРСТ
Ф	фхцчшщъыьэюяАБВГДЕЖЗИЙКЛМНОПРСТУ
Х	хцчшщъыьэюяАБВГДЕЖЗИЙКЛМНОПРСТУФ
Ц	цчшщъыьэюяАБВГДЕЖЗИЙКЛМНОПРСТУФХ
Ч	чшщъыьэюяАБВГДЕЖЗИЙКЛМНОПРСТУФХЦ
Ш	шщъыьэюяАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧ
Щ	щъыьэюяАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШ
Ъ	ъыьэюяАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩ
Ы	ыьэюяАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪ
Ь	ьэюяАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫ
Э	эюяАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬ
Ю	юяАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭ
Я	яАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮ

*Примечание***.** Шифр Виженера представляет собой многоалфавитную (полиалфавитную) систему шифрования. Идея шифра состоит в использовании в качестве ключа (кодовое слово) текста самого сообщения (открытого – не зашифрованного) или же шифрованного текста (закрытого). Для усиления стойкости шифра, в качестве первого символа ключа возможно взять случайным образом букву из алфавита. В общем случае таблица Виженера состоит из алфавита, циклически сдвинутого на один символ влево, однако возможны и другие перестановки. Первая строка может представлять собой алфавит, случайным образом перемешанный.

Открытый текст, который надо зашифровать, записывается в строку без пробелов (возможно использование пробела, если это предусмотрено таблицей Виженера). Далее

необходимо определить ключ. Виженер предлагал в качестве ключа использовать сам открытый текст, с добавлением к началу ключа символа, выбранного случайным образом. Однако, не обязательно следовать установленному правилу создателя шифра. В качестве ключа вполне возможно использовать и любую другую последовательность символов.

ТЕСТОВЫЕ ЗАДАНИЯ ДЛЯ САМОПОДГОТОВКИ

1. Основные угрозы доступности информации:

а) непреднамеренные ошибки пользователей

б) злонамеренное изменение данных

в) хакерская атака

г) отказ программного и аппаратного обеспечения

д) разрушение или повреждение помещений

е) перехват данных.

2. Суть компрометации информации:

а) внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации

б) несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений

в) внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений.

3. Информационная безопасность автоматизированной (компьютерной) системы – это состояние автоматизированной системы, при котором она, ...

а) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой - ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды

б) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации

в) способна противостоять только информационным угрозам, как внешним так и внутренним

г) способна противостоять только внешним информационным угрозам.

4. Методы повышения достоверности входных данных:

а) замена процесса ввода значения процессом выбора значения из предлагаемого множества

б) отказ от использования данных

в) проведение комплекса регламентных работ

г) использование вместо ввода значения его считывание с машиночитаемого носителя

д) введение избыточности в документ первоисточник

е) многократный ввод данных и сличение введенных значений.

5. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ):

а) МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения

б) МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты

в) МЭ работают только на сетевом уровне, а СОВ – еще и на физическом.

6. Сервисы безопасности:

а) идентификация и аутентификация

б) шифрование

в) инверсия паролей

г) контроль целостности

д) регулирование конфликтов

е) экранирование

ж) обеспечение безопасного восстановления

и) кэширование записей.

7. Под угрозой удаленного администрирования в компьютерной сети понимается угроза ...

а) несанкционированного управления удаленным компьютером

б) внедрения агрессивного программного кода в рамках активных объектов Web-страниц

в) перехвата или подмены данных на путях транспортировки

г) поставки неприемлемого содержания.

8. Причины возникновения ошибки в данных:

а) погрешность измерений

б) ошибка при записи результатов измерений в промежуточный документ

в) неверная интерпретация данных

г) ошибки при переносе данных с промежуточного документа в компьютер

д) использование недопустимых методов анализа данных

е) неустранимые причины природного характера

ж) преднамеренное искажение данных

и) ошибки при идентификации объекта или субъекта хозяйственной деятельности.

9. К формам защиты информации не относится...

а) аналитическая

б) правовая

в) организационно-техническая

г) страховая.

10. Наиболее эффективное средство для защиты от сетевых атак:

а) использование сетевых экранов или «firewall»

б) использование антивирусных программ

в) посещение только «надёжных» Интернет-узлов

г) использование только сертифицированных программ-браузеров при доступе к сети Интернет.

11. Информация, составляющая государственную тайну, не может иметь гриф...

а) «для служебного пользования»

б) «секретно»

в) «совершенно секретно»

г) «особой важности».

12. Разделы современной криптографии:

а) Симметричные криптосистемы

б) Криптосистемы с открытым ключом

в) Криптосистемы с дублированием защиты

г) Системы электронной подписи

д) Управление паролями

е) Управление передачей данных

ж) Управление ключами.

13. Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности:

а) рекомендации X.800

б) Оранжевая книга

в) Закон «Об информации, информационных технологиях и о защите информации».

14. Утечка информации – это ...

а) несанкционированный процесс переноса информации от источника к злоумышленнику

б) процесс раскрытия секретной информации

в) процесс уничтожения информации

г) непреднамеренная утрата носителя информации.

15. Основные угрозы конфиденциальности информации:

а) маскарад

б) карнавал

в) переадресовка

г) перехват данных

д) блокирование

е) злоупотребления полномочиями.

16. Элементы знака охраны авторского права:

а) буквы С в окружности или круглых скобках

б) буквы Р в окружности или круглых скобках

в) наименования (имени) правообладателя

г) наименование охраняемого объекта

д) года первого выпуска программы.

17. Защита информации обеспечивается применением антивирусных средств

а) да

б) нет

в) не всегда.

18. Средства защиты объектов файловой системы основаны на…

а) определении прав пользователя на операции с файлами и каталогами

б) задании атрибутов файлов и каталогов, независящих от прав пользователей.

19. Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование - ... угроза

а) активная

б) пассивная.

20. Преднамеренная угроза безопасности информации:

а) кража

б) наводнение

в) повреждение кабеля, по которому идет передача, в связи с погодными условиями

г) ошибка разработчика.

21. Концепция системы защиты от информационного оружия не должна включать…

а) средства нанесения контратаки с помощью информационного оружия

б) механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры

в) признаки, сигнализирующие о возможном нападении

г) процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей.

22. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на ...

а) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации

б) реализацию права на доступ к информации

в) соблюдение норм международного права в сфере информационной безопасности

г) выявление нарушителей и привлечение их к ответственности

д) соблюдение конфиденциальности информации ограниченного доступа

е) разработку методов и усовершенствование средств информационной безопасности.

23. Компьютерные вирусы - это:

а) вредоносные программы, которые возникают в связи со сбоями в аппаратных средствах компьютера

б) программы, которые пишутся хакерами специально для нанесения ущерба пользователям ПК

в) программы, являющиеся следствием ошибок в операционной системе

г) вирусы, сходные по природе с биологическими вирусами.

24. Что не относится к объектам информационной безопасности РФ?

а) природные и энергетические ресурсы

б) информационные системы различного класса и назначения, информационные технологии

в) система формирования общественного сознания

г) права граждан, юридических лиц и государства на получение, распространение, использование и защиту информации и интеллектуальной собственности.

25. Какие действия в Уголовном кодексе РФ классифицируются как преступления в компьютерной информационной сфере?

а) неправомерный доступ к компьютерной информации

б) создание, использование и распространение вредоносных программ для ЭВМ

в) умышленное нарушение правил эксплуатации ЭВМ и их сетей

г) все перечисленное выше.

26. Политика безопасности:

а) фиксирует правила разграничения доступа

б) отражает подход организации к защите своих информационных активов

в) описывает способы защиты руководства организации.

27. При анализе стоимости защитных мер следует учитывать:

а) расходы на закупку оборудования

б) расходы на закупку программ

в) расходы на обучение персонала.

28. Протоколирование и аудит могут использоваться для:

а) предупреждения нарушений ИБ

б) обнаружения нарушений

в) восстановления режима ИБ

29. Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами:

а) выработка и проведение в жизнь единой политики безопасности

б) унификация аппаратно-программных платформ

в) минимизация числа используемых приложений.

30.Экранирование может использоваться для:

а) предупреждения нарушений ИБ

б) обнаружения нарушений

в) локализации последствий нарушений.

31. В число основных принципов архитектурной безопасности входят:

а) следование признанным стандартам
б) применение нестандартных решений, не известных злоумышленникам
в) разнообразие защитных средств.

32. В число основных принципов архитектурной безопасности входят:

а) усиление самого слабого звена
б) укрепление наиболее вероятного объекта атаки
в) эшелонированность обороны.

33. Риск является функцией:

а) размера возможного ущерба
б) числа пользователей ИС
в) уставного капитала организации.

34. Первый шаг в анализе угроз – это:

а) идентификация угроз
б) аутентификация угроз
в) ликвидация угроз.

35. Управление рисками включает в себя следующие виды деятельности:

а) определение ответственных за анализ рисков
б) оценка рисков
в) выбор эффективных защитных средств.

36. Цифровой сертификат содержит:

а) открытый ключ пользователя
б) секретный ключ пользователя
в) имя пользователя.

37. Криптография необходима для реализации следующих сервисов безопасности:

а) контроль конфиденциальности
б) контроль целостности
в) контроль доступа.

38. Экран выполняет функции:

а) разграничения доступа
б) облегчения доступа
в) усложнения доступа.

39. Демилитаризованная зона располагается:

а) перед внешним межсетевым экраном
б) между межсетевыми экранами
в) за внутренним межсетевым экраном.

40. Криптография необходима для реализации следующих сервисов безопасности:

а) идентификация
б) экранирование
в) аутентификация.

41. Экранирование на сетевом и транспортном уровнях может обеспечить:

а) разграничение доступа по сетевым адресам
б) выборочное выполнение команд прикладного уровня
в) контроль объема данных, переданных по TCP-соединению.

42. Туннелирование может использоваться на следующем уровне модели OSI:

а) сетевом
б) сеансовом
в) уровне представления.

43. Принцип усиления самого слабого звена можно переформулировать как:

а) принцип равнопрочности обороны

б) принцип удаления слабого звена

в) принцип выявления главного звена, ухватившись за которое можно вытянуть всю цепь.

44. Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности:

а) просчеты при администрировании ИС

б) необходимость постоянной модификации ИС

в) сложность современных ИС

45. Для внедрения бомб чаще всего используются ошибки типа:

а) отсутствие проверок кодов возврата

б) переполнение буфера

в) нарушение целостности транзакций.

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1. Сущность информационных рисков. Определение (понятие «информационный риск»).
2. Прямые и косвенные информационные риски. Причина, фактор и источник риска. Основные направления управления информационными рисками.
3. Анализ информационных рисков.
4. Построение системы управления информационными рисками (СУИР). Принципы построения СУИР.
5. Информация как объект защиты. Свойства информации как объекта защиты.
6. Программа и стратегии управления информационными рисками предприятия.
7. Схема управления информационными рисками с учетом выбора стратегии управления информационными рисками.
8. Понятие «угрозы безопасности информации». Классификация угроз безопасности информации.
9. Внешние и внутренние угрозы безопасности информации. Случайные и преднамеренные угрозы. Приведите примеры.
10. Методы традиционного шпионажа и диверсий. Приведите примеры.
11. Современные средства прослушивания и принципы их действия. Приведите примеры.
12. Современные средства визуального наблюдения (видеоразведка). Приведите примеры.
13. Понятие «несанкционированный доступ к информации» (НСДИ). Система разграничения доступа к информации. Каналы НСДИ.
14. Несанкционированная модификация технической и программной структуры компьютерной информационной системы (КС). Недекларированные возможности КС. Аппаратные и программные закладки.
15. Угрозы безопасности информации в распределенных системах.
16. Классификация злоумышленников. Технологические возможности злоумышленников по преодолению систем защиты информации.
17. Характеристика физических каналов негативного воздействия на ИР. Последствия воздействия.
18. Правовое регулирование в области безопасности информации. Задачи государства в данной области.
19. Основные положения Доктрины информационной безопасности Российской Федерации.

20. Характеристика основных законов РФ, регулирующих отношения в области ИТ.

21. Стандарты как механизм управления информационными рисками. Виды стандартов. Приведите примеры.

22. Организационная структура системы обеспечения информационной безопасности Российской Федерации. Государственные органы, обеспечивающие безопасность ИТ и решаемые ими задачи.

23. Организационные методы обеспечения информационной безопасности предприятия и их характеристика. Приведите примеры.

24. Направления защиты от случайных угроз и их характеристика.

25. Приведите характеристику дублирования информации в КС. Методы дублирования информации (оперативные и неоперативные; сосредоточенное и рассредоточенное и др.) их возможности и недостатки.

26. Понятие репликации и резервного копирования, их отличия. Технология RAID.

27. Пути повышения надежности и отказоустойчивости КС. Основные подходы к созданию отказоустойчивых систем.

28. Защита от ошибок: блокировка ошибочных операций и направления оптимизации взаимодействия пользователя с КС.

29. Противодействие техногенным авариям и стихийным бедствиям. Минимизация ущерба от аварий и стихийных бедствий.

30. Система охраны информационных объектов, ее состав и характеристика компонентов системы.

31. Характеристика технических возможностей современных инженерных конструкций, систем сигнализации, средств наблюдения, подсистем доступа на объекты.

32. Структура типовой системы охранной сигнализации и ее структура. Принцип действия элементов охранной сигнализации.

33. Структурная схема телевизионной системы видеоконтроля. Устройства обработки и коммутации видеоинформации.

34. Понятия «идентификация» и «аутентификация». Средства и методы идентификации и аутентификации субъектов доступа.

35. Организация работы с документацией на предприятиях.

36. Механизмы противодействия ведению видеоразведки, прослушиванию в помещениях и при использовании коммуникационного оборудования.

37. Характеристика методов защиты от прослушивания акустических сигналов.

38. Средства борьбы с закладными подслушивающими устройствами и их характеристики.

39. Методы борьбы с инсайдерами.

40. Модели доступа. Защита информации в компьютерных системах от несанкционированного доступа (НСД).

41. Система разграничения доступа к информации и ее структура.

42. Приведите сравнительную характеристику матричного и мандатного методов доступа.

43. Перечислите основные способы неявного задания матрицы доступа и охарактеризуйте их.

44. Средства ОС и MS Office по защите от несанкционированного доступа к документам.

45. Разграничение доступа к информации в базах данных.

46. Методы и средства защиты от несанкционированного изменения структур компьютерных систем. Приведите примеры.

47. Приведите основные возможности OS Windows по разграничению доступа.

48. Приведите основные возможности по разграничению доступа в приложениях MS Office.

49. Методы скрытия информации. Методы стеганографии.

50. Основные понятия криптографии.

51. Классификация методов шифрования. Требования к современным шифрам.

52. Методы симметричного шифрования. Блочное и потоковое шифрование.

53. Несимметричное шифрование. Абсолютно надежный шифр.

54. Особенности защиты информации в распределенных КС.

55. Основные понятия информационной защиты сети. Средства защиты сетей. Протокол Керберос. Защита по протоколу Керберос.

56. Защита информации в каналах связи. Приведите примеры.

57. Межсетевое экранирование. Принцип действия схем защиты с помощью брандмауэров (межсетевые экраны).

58. Системы дистанционного банковского обслуживания, принципы и схема их функционирования. Обеспечение информационной безопасности процессов функционирования систем дистанционного банковского обслуживания.

59. Системы электронной торговли, принципы и схема их функционирования. Обеспечение информационной безопасности процессов функционирования систем электронной торговли.

60. Методы и средства обеспечения безопасной работы в сети Интернет.

61. Классификация компьютерных вирусов и вредоносных программ. Приведите примеры.

62. Методы и средства борьбы с компьютерными вирусами и вредоносными программами.

63. Профилактика заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения.