МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(ДГТУ)

Кафедра «Вычислительные системы и информационная безопасность»

Методические рекомендации по изучению дисциплины «Техническая защита информации в информационных системах» для обучающихся 1-го курса по направлению 09.04.02 Информационные системы и технологии заочной формы обучения (классификация – магистр)

Ростов – на – Дону
2023г.

Составители:
Н.Д. Панасенко

УДК 004

Подготовлено на кафедре «Вычислительные системы и информационная безопасность»

Методические рекомендации
к контрольной работе дисциплины «**Техническая защита информации в информационных системах»**
/ ДГТУ, Ростов – на – Дону, 2023

Методические рекомендации по изучению дисциплины для обучающихся представляют собой комплекс рекомендаций и разъяснений, позволяющих обучающимся оптимальным образом организовать процесс изучения данной дисциплины. Методические рекомендации могут быть использованы для самостоятельной работы. Позволяет обучающимся оптимальным образом организовать процесс выполнения контрольной работы.

ВВЕДЕНИЕ

Цели и задачи дисциплины

Подготовка обучающихся к деятельности, связанной с использованием различных современных средств защиты информации, а также формирование представлений о разработке, реализации, эксплуатации, анализе, сопровождения и совершенствования систем управления информационной безопасностью компьютерных систем.

Задачи дисциплины:

– знать физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; номенклатуру и характеристики аппаратуры, используемой для съема, перехвата и анализов сигналов в технических каналах утечки информации; основные методы и средства технической защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съёма и утечки по техническим каналам.;

– научить обучающихся оценивать степень защищенности информации автоматизированной системы и потенциально возможные действия злоумышленника;

– научить обучающихся применять технические средства защиты информации; использовать средства защиты информации от несанкционированного съёма и утечки по техническим каналам; применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности техническими средствами.

1. Алгоритм выбора варианта контрольной работы

Для выбора варианта контрольной работы необходимо взять предпоследнюю и последнюю цифры номера зачетной книжки. Номер варианта находится на пересечении соответствующей строки и столбца.

	Последняя цифра номера зачетной книжки										
		0	1	2	3	4	5	6	7	8	9
Предпоследняя цифра номера зачетной книжки	0	1	8	4	6	1	5	3	8	7	1
	1	8	2	7	5	3	2	1	3	2	8
	2	3	7	3	6	4	1	6	3	7	1
	3	7	4	1	4	5	3	4	4	8	6
	4	4	8	6	8	5	5	5	1	5	8
	5	2	6	7	1	6	6	4	6	6	2
	6	5	2	5	7	3	1	7	3	7	6
	7	3	5	8	2	4	7	5	8	2	3
	8	6	1	1	3	8	2	6	4	1	1
	9	2	1	4	2	2	5	8	3	4	2

Например, для зачетки с номером 123456 необходимо взять номер варианта из 5 – ой строки и 6 – го столбца (вариант 4).

2. Задания для выполнения контрольной работы

При выполнении контрольной работы необходимы компьютеры с установленной ОС Windows, пакет Microsoft Office. К полученной контрольной работе прилагать выполненные работы в электронном виде на цифровом носителе.

Работа № 1.
Написать реферат на одну из нижеперечисленных тем в соответствии с вариантом (оформление согласно правилам вуза)

1. Оценка качества параметров технической защиты объекта на основе моделей из вычислительной геометрии.
2. Техническая защита речевой информации на каналах связи сети общего пользования.
3. Техническая разведка как угроза безопасности информации органов внутренних дел (ОВД).
4. Инженерно-техническая защита информации как сфера научной и практической деятельности.
5. Техническая защита информации с помощью инженерных средств.
6. Защита информации с помощью технических систем охранно-пожарной сигнализации.
7. Защита информации с помощью технических систем управления доступом.
8. Понятие и классификация технических мер защиты информации.

Работа №2.
Оценить информационные ресурсы. Привести полученные результаты создания в виде рисунков, таблиц, как второе задание реферата (оформленного согласно правилам вуза)

Цель работы: формирование у обучающихся навыка работы с нормативными документами по исследуемому вопросу и умение анализа угроз информационной безопасности.

Задание:

1. оценить информационные ресурсы;
2. выявить косвенные факторы, влияющие на выполнение уязвимостей и составить перечень их параметров;
3. оценить информационные риски.

Оценка информационных ресурсов производится следующим образом:

1) определяется состав параметров, влияющих на стоимость ресурса.

2) количественные значения приводятся в безразмерный вид. Для этого текущее значение параметра необходимо разделить на его максимальное значение.

3) значения параметров складываются. Для выполнения второй задачи, необходимо рассмотреть угрозы и уязвимости в информационной системе предприятий. При этом использовать предприятие (модель предприятия) выбранное самостоятельно. Методика выявления факторов и их показателей изложена выше.

Каждое крупное предприятие требует детального изучения возможных угроз. В каждом конкретном случае требуется свое решение. В то же время есть много общего.

Оценка рисков, производится в соответствии с формулами (1) и (2).

Оценку информационных ресурсов (таблица 1).

Необходимо провести анализ защищенности объекта защиты информации по следующим разделам:

- виды возможных угроз;
- характер происхождения угроз;
- классы каналов несанкционированного получения информации;

– источники появления угроз;
– причины нарушения целостности информации;
– потенциально возможные злоумышленные действия;
– определить класс защищенности автоматизированной системы.

Перечень параметров уязвимостей системы разместить в таблице 2.

Оценку информационных рисков (таблица 3).

Таблица 1 – Оценка стоимости ресурса

№ п.п.	Наименование ресурса	Параметры	Значение	Приведенное значение

Таблица 2 – Перечень параметров уязвимости системы

№ п.п.	Факторы	Уязвимости	Значение

Таблица 3 – Оценка рисков информационной безопасности

№ п.п.	Уязвимость	Риск

Теоретические сведения

Понятие «информационная безопасность» (ИБ) рассматривается как состояние защищенности потребностей личности, общества и государства в информации, при котором обеспечиваются их существование и прогрессивное развитие независимо от наличия внутренних и внешних информационных угроз. Тогда с позиции обеспечения ИБ можно определить, что под информационной угрозой понимается воздействие дестабилизирующих факторов на состояние информированности, подвергающее опасности жизненно важные интересы личности, общества и государства.

В законе РФ «О безопасности» дано определение угрозы безопасности как совокупности условий, факторов, создающих опасность жизненно важным интересам личности, общества и государства. Под угрозой информации в

системах ее обработки понимается возможность возникновения на каком -либо этапе жизнедеятельности системы такого явления или события, следствием которого могут быть нежелательные воздействия на информацию. К настоящему времени известно большое количество разноплановых угроз различного происхождения, таящих в себе различную опасность для информации. Для системного представления их удобно классифицировать по виду, возможным источникам, предпосылкам появления и характеру проявления.

Виды угроз

Определив понятие «угроза государству, обществу и личности» в широком смысле, рассмотрим его относительно не посредственного воздействия на конфиденциальную информацию, обрабатываемую на каком-либо объекте (кабине те, предприятии, фирме). Анализируя возможные пути воздействия на информацию, представляемую как совокупность информационных элементов, связанных между собой логическими связями (рисунок 1), можно выделить основные нарушения:

— физической целостности (уничтожение, разрушение элементов);

— логической целостности (разрушение логических связей);

— содержания (изменение блоков информации, внешнее навязывание ложной информации);

— конфиденциальности (разрушение защиты, уменьшение степени защищенности информации),

— прав собственности на информацию (несанкционированное копирование, использование).

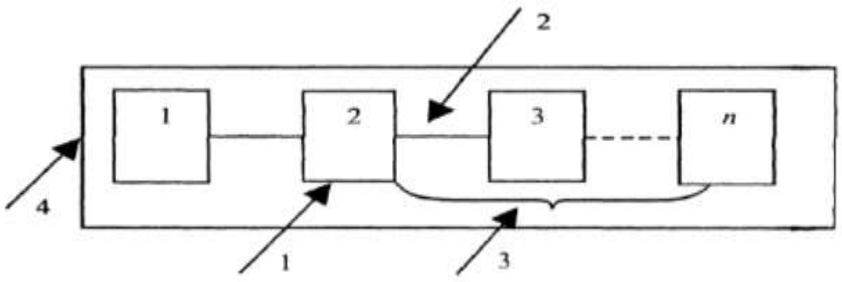

Рисунок 1 – Возможные пути воздействия на информацию

С учетом этого для таких объектов систем угроза информационной безопасности представляет реальные или потенциально возможные действия или

условия, приводящие к овладению конфиденциальной информацией, хищению, искажению, изменению, уничтожению ее и сведений о самой системе, а также к прямым материальным убыткам.

Обобщая рассмотренные угрозы, можно выделить три наиболее выраженные для систем обработки информации:

1) подверженность физическому искажению или уничтожению;

2) возможность несанкционированной (случайной или злоумышленной) модификации;

3) опасность несанкционированного (случайного или преднамеренного) получения информации лицами, для которых она не предназначалась.

Кроме того, с точки зрения анализа процесса обработки информации выделяют такую угрозу, как блокирование доступа к обрабатываемой информации.

Характер происхождения угроз

Угрозы безопасности информации в современных системах ее обработки определяются умышленными (преднамеренные угрозы) и естественными (непреднамеренные угрозы) разрушающими и искажающими воздействиями внешней среды, надежностью функционирования средств обработки информации, а также преднамеренным корыстным воздействием несанкционированных пользователей, целями которых являются хищение, уничтожение, разрушение, несанкционированная модификация и использование обрабатываемой информации. При этом под умышленными, или преднамеренными, понимаются такие угрозы, которые обусловливаются злоумышленными действиями людей. Случайными, или естественными, являются угрозы, не зависящие от воли людей. В настоящее время принята следующая классификация угроз сохранности (целостности) информации (рисунок 2).

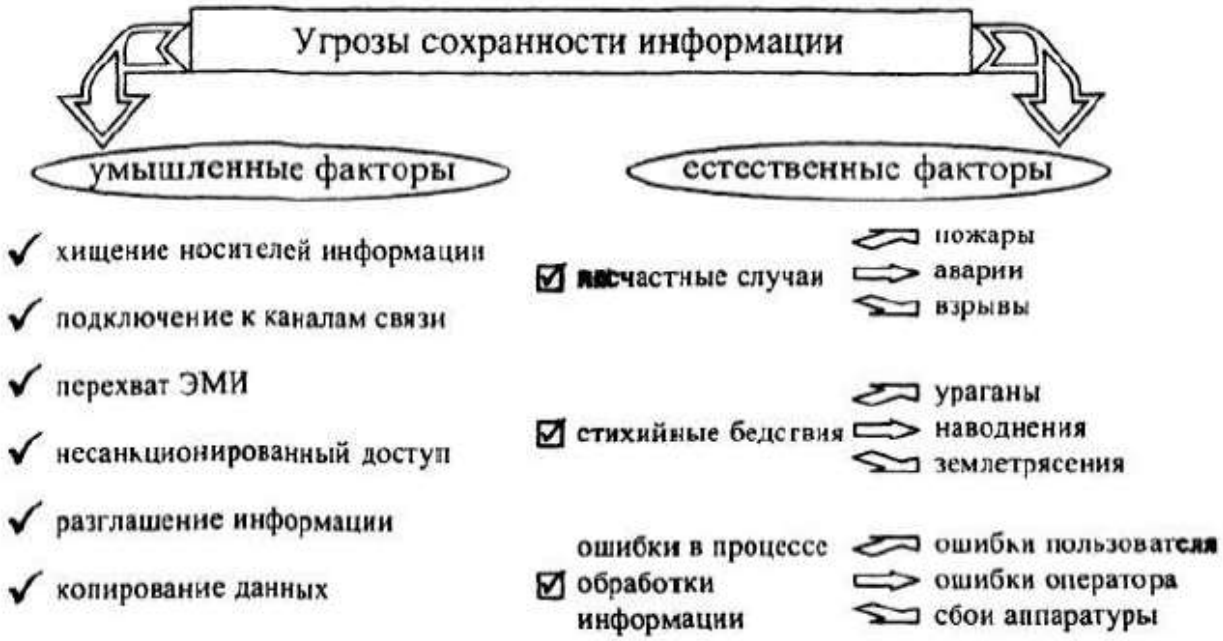

Рисунок 2 – Классификация угроз целостности информации

Источники угроз

Под источником угроз понимается непосредственный исполнитель угрозы с точки зрения ее негативного воздействия на информацию. Источники можно разделить на следующие группы:

— люди;

— технические устройства;

— модели, алгоритмы, программы;

— технологические схемы обработки;

— внешняя среда

Предпосылки появления угроз

Существуют следующие предпосылки, или причины, появления угроз:

— объективные (количественная или качественная недостаточность элементов системы) – не связанные непосредственно с деятельностью людей и вызывающие случайные по характеру происхождения угрозы;

— субъективные – непосредственно связанные с деятельностью человека и вызывающие как преднамеренные (деятельность разведок иностранных государств, промышленный шпионаж, деятельность уголовных элементов и недобросовестных сотрудников), так и непреднамеренные (плохое

психофизиологическое состояние, недостаточная подготовка, низкий уровень знаний) угрозы информации.

Взаимодействие угроз можно представить на рисунке 3

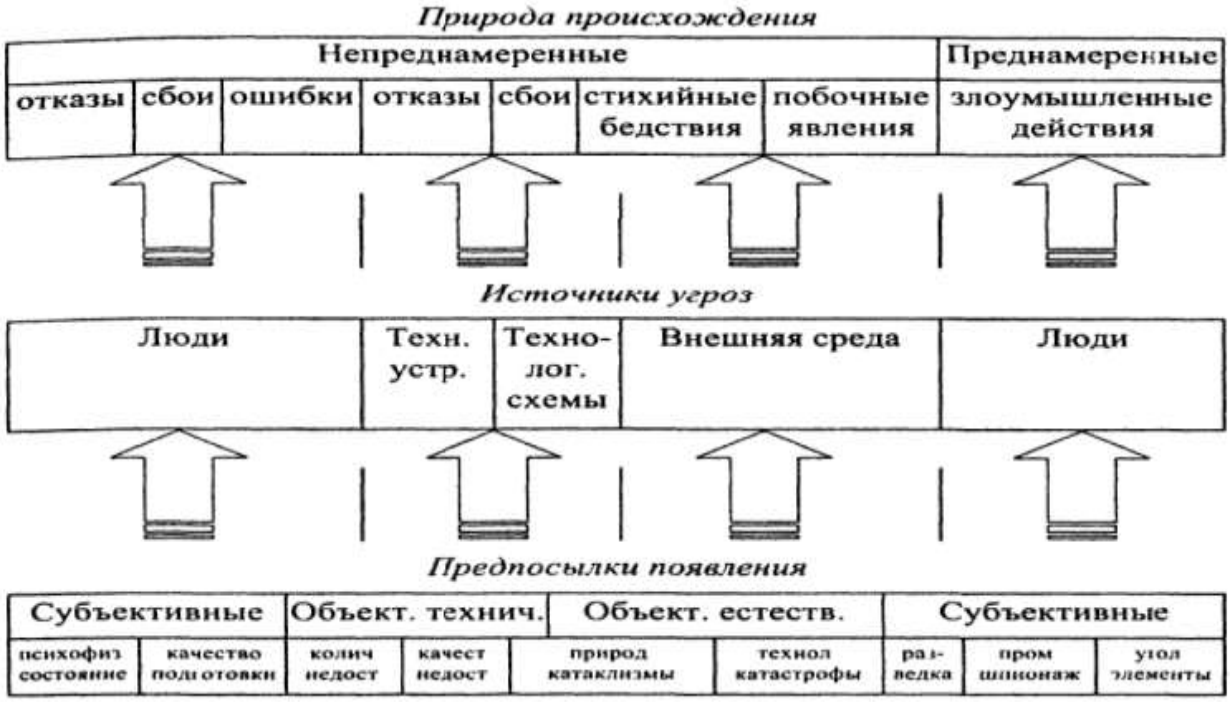

Рисунок 3 – Взаимодействие параметров угроз информации

Перечисленные разновидности предпосылок интерпретируются следующим образом:

— количественная недостаточность — физическая не хватка одного или нескольких элементов системы обработки, вызывающая нарушения технологического процесса обработки или перегрузку имеющихся элементов;

— качественная недостаточность — несовершенство конструкции (организации) элементов системы, в силу чего может появляться возможность случайного или преднамеренного негативного воздействия на обрабатываемую или хранимую ин формацию;

— деятельность разведорганов иностранных государств — специально организуемая деятельность государственных органов разведки, профессионально ориентированных на добывание необходимой информации всеми доступными способами и средствами;

— промышленный шпионаж: — негласная деятельность отечественны х и зарубежных промышленных организаций (фирм), направленная на по лучение

незаконным путем конфиденциальной информации, используемой для достижения промышленных, коммерческих, политических или подрывных целей;

— злоумышленные действия уголовных элементов — хищение информации, средств ее обработки или компьютерных программ в целях наживы или их разрушение в интересах конкурентов;

— плохое психофизиологическое состояние — постоянное или временное психофизиологическое состояние сотрудников, приводящее при определенных нестандартных внешних воздействиях к увеличению ошибок и сбоев в обслуживании систем обработки информации или непосредственно к разглашению конфиденциальной информации;

— недостаточная качественная подготовка сотрудников — уровень теоретической и практической подготовки персонала к выполнению задач по защите информации, недостаточная степень которого может привести к нарушению процесса функционирования системы защиты информации.

В современной литературе и нормативно-правовых актах в области информационной безопасности можно встретить такую классификацию угроз информации, которая делит их на внутренние и внешние. Одной из наиболее принципиальных особенностей проблемы защиты информации является формирование полного множества угроз информации, потенциально возможных на объекте ее обработки. В самом деле, даже одна неучтенная угроза может в значительной мере снизить эффективность защиты.

Возможные пути получения конфиденциальной информации

Анализ рассмотренных видов угроз позволяет сгруппировать их по двум основным областям:

1) угрозы нарушения физической и логической целостности, а также содержания информации (несанкционированная модификация). Их можно объединить в причины нарушения целостности информации (ПНЦИ);

2) угрозы, следствием которых может быть получение защищаемой информации (хищение или копирование) лицами, не имеющими на это полномочий, — в каналы несанкционированного получения информации (КНПИ).

Под действием рассмотренных выше угроз может произойти утечка защищаемой информации, то есть несанкционированное, неправомерное завладение соперником данной информацией и возможность использования ее в своих, в ущерб интересам собственника (владельца) информации, целях. При этом образуется канал утечки информации, под которым понимается физический путь от источника конфиденциальной информации к злоумышленнику. Для его возникновения необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства восприятия и фиксации информации на стороне злоумышленника.

В зависимости от используемых соперником сил и средств для получения несанкционированного доступа к носителям защищаемой информации различают каналы агентурные, технические, легальные.

Агентурные каналы утечки информации — это использование противником тайных агентов для получения несанкционированного доступа к носителям защищаемой информации. В случае использования агентами технических средств разведки (направленных микрофонов, закладных устройств, миниатюрных видеокамер и др.) говорят о ведении агентурно-технической разведки.

Технические каналы утечки информации — совокупность технических средств разведки, демаскирующих признаков объекта защиты и сигналов, несущих информацию об этих признаках.

Эти каналы образуются без участия человека в процессе обработки информации техническими средствами, а поэтому являются одними из наиболее опасных и требуют отдельного рассмотрения.

Легальные каналы утечки информации — это использование соперником открытых источников информации (литературы, периодических изданий и т. п), обратный инжиниринг, выведывание под благовидным предлогом информации у лиц, располагающих интересующей соперника информацией, и других возможностей. В основу классификации ПНЦИ положен показатель, характеризующий степень участия в этом процессе человека. В соответствии с

таким подходом ПНЦИ делятся на два вида (объективные и субъективные) и на следующие классы (рисунок 4).

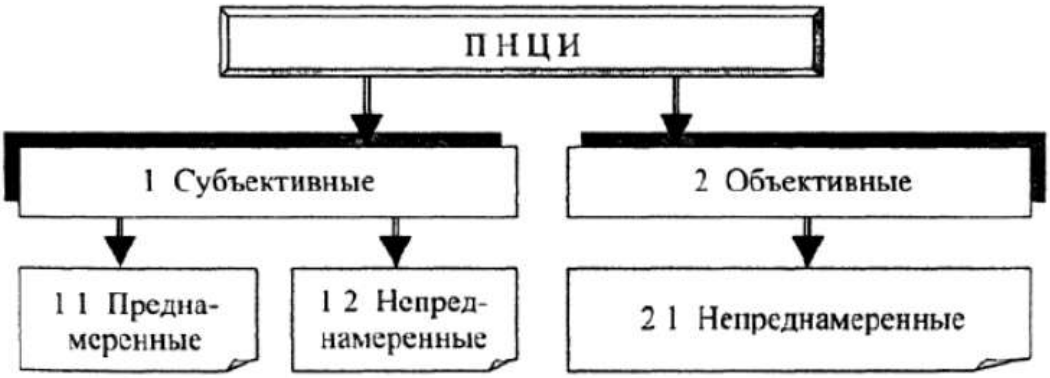

Рисунок 4 – Классификация ПНЦИ

1.1. Субъективные преднамеренные.

1.1.1. Диверсия (организация пожаров, взрывов, повреждение электропитания и др.).

1.1.2. Непосредственные действия над носителем (хищение, подмена носителей, уничтожение информации).

1.1.3. Информационное воздействие (электромагнитное облучение, ввод в компьютерные системы разрушающих программных средств, воздействие на психику личности психотропным оружием).

1.2. Субъективные непреднамеренные.

1.2.1. Отказы обслуживающего персонала (гибель, длительный выход из строя).

1.2.2. Сбои людей (временный выход из строя).

1.2.3. Ошибки людей.

2.1. Объективные непреднамеренные.

2.1.1. Отказы (полный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения.

2.1.2. Сбои (кратковременный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения.

2.1.3. Стихийные бедствия (наводнения, землетрясения, ураганы).

2.1.4. Несчастные случаи (пожары, взрывы, аварии).

2.1.5. Электромагнитная несовместимость.

Для предотвращения возможной утечки конфиденциальной информации и нарушения ее целостности на объектах ее обработки разрабатывается и внедряется система защиты информации. Система защиты информации — совокупность взаимосвязанных средств, методов и мероприятий, направленных на предотвращение уничтожения, искажения, несанкционированного получения конфиденциальных сведений, отображенных физическими полями, электромагнитными, световыми и звуковыми волнами или вещественно-материальными носителями в виде сигналов, образов, символов, технических решений и процессов.

При построении комплексных систем защиты информации зачастую трудно определить уровень различных угроз безопасности. Это может привести к неадекватным мерам по их нейтрализации. Для избежание подобных ситуаций необходима количественная оценка степени влияния угроз безопасности информации на информационную систему.

Целью анализа рисков является количественная оценка угроз и уязвимостей, позволяющая определить комплекс контрмер, обеспечивающий достаточный уровень защищенности информационной системы.

При проведении оценки рисков необходимо иметь чёткое представление таких понятий, угроза информационной безопасности и уязвимость информационной системы или системы защиты информации.

Угроза – совокупность условий и факторов, которые могут стать причиной снижения заданного уровня безопасности информации.

Уязвимость – слабость в системе защиты, которая делает возможным реализацию угрозы.

Риск нарушения ИБ – возможность реализации угрозы.

Величину риска можно определить, исходя из следующей формулы:

$$P = C \times P_y, \quad (1)$$

где P – величина риска, C – стоимость информационного ресурса, P_y – вероятность реализации угрозы.

Стоимость информационного ресурса – это количественная величина, характеризующая степень влияния данного ресурса на информационную систему. Его можно определить как уровень потерь, понесённых владельцами ресурса или информационной системой при его утрате или разглашении. В зависимости от реальных условий, стоимость может быть выражена либо в деньгах, либо условных единицах.

Вероятность реализации угрозы зависит от множества факторов. Основными из них будут:

– наличие самой угрозы;

– наличие и вероятность реализации уязвимостей системы;

– привлекательности уязвимости.

В рамках проведения данной работы условимся не учитывать привлекательность той или иной уязвимости. Поскольку наличие угрозы может зависеть от субъективных факторов, например, желания злоумышленника реализовать угрозу, условимся не учитывать и этот фактор. Таким образом, примем вероятность реализации угрозы P_y равной вероятности реализации уязвимости.

Вероятность реализации угрозы можно рассчитать, исходя из следующей формулы:

$$P_y = P_s \times P_t \times P_p, \quad (2)$$

где P_s – пространственное условие, т.е. вероятность того, что угроза реализуется в том месте, где находится информация; P_t – временное условие, т.е. вероятность того, что угроза реализуется в тот момент, когда информация существует; P_p – энергетическое условие реализации угрозы, т.е. вероятность того, что энергии, для выполнения уязвимости будет достаточно.

Перечисленные условия являются *основными факторами* выполнения уязвимости. Т.е. при невыполнении хотя бы одного из них уязвимость реализовать невозможно. Однако эти условия сами зависят от множества факторов. Факторы, от которых зависит выполнимость основных называются *косвенными.* Состав косвенных факторов, характер их влияния на основные

заранее определить невозможно. Поэтому значения вероятностей наступления основных факторов будут вычисляться из значений вероятности наступления косвенных для каждого конкретного случая отдельно.

При вычислении значений основных факторов необходимо помнить, что это вероятностные характеристики и вычисляются по правилам теории вероятности. Таким образом, если основной фактор зависит от одного показателя (косвенного фактора) – *расчет по одному критерию*, то находится он, как отношение величины критерия к его максимальному значению. Проще говоря, меньшее необходимо разделить на большее. О правильности выбора и расчёта вероятности можно судить исходя из простого правила – *значение вероятности всегда должно быть меньше 1*.

Если значение вероятности наступления основного фактора зависит от нескольких критериев, то расчет может производится либо по *суммовым*, либо по *критическим* критериям. Суммовыми будут критерии, которые вносят определенную долю в вероятность наступления фактора и не зависят друг от друга. При этом необходимо вычислить вероятность наступления каждого из косвенных факторов методом расчета по одному критерию, а затем сложить их, используя следующую формулу:

$$P_{оф} = \sum_{i}^{n} P_i - \prod_{i}^{n} P_i , \qquad (3)$$

где $P_{оф}$ – вероятность наступления основного фактора; P_i – вероятность наступления косвенного фактора; i – индекс фактора; n – количество факторов.

Критические – это критерии, которые зависят друг от друга. Т.е. такие критерии, от значения каждого из которых зависит наступление события. Вероятностные показатели этих критериев необходимо перемножить:

$$P_{оф} = \prod_{i}^{n} P_i . \qquad (4)$$

Рассмотри теперь что же является, собственно, самими косвенными факторами и их критериями. *Косвенным фактором* может являться всё, что может привести к реализации угрозы через уязвимость. А критерием является

количественный показатель, по которому можно вычислить вероятность наступления этого события.

Например, для бумажного документа, косвенным фактором будет время его хранения. Точнее вероятность утери документа за это время. А критериями этого события могут быть: объем документа (количество листов), температурно-влажностный режим в месте хранения, вероятность кражи и т.д. Для электронной информационной базы данных – объём “винчестера” (или томов), скорость передачи в ЛВС, мощность или быстродействие микропроцессора, объем оперативной памяти и т.д.

Все эти показатели могут быть 3-х типов: технические, статистические и приведённые.

Технические – это показатели, имеющие свои единицы измерения. Такие показатели, как правило, относятся к характеристикам технических устройств. Они имеют четкое значение в каждый момент времени, область определения или максимальное значение. Определение вероятности наступления неблагоприятного события по этим показателям является наиболее простым.

Например, чтобы определить вероятность разрушения базы данных на “винчестере”, необходимо объём базы данных разделить на полный объём “винчестера”.

Статистические – это показатели, которые можно определить исходя из статистической информации. Ярким примером служит такой показатель, как время наработки на отказ. Этот показатель определяется в период эксплуатации технического устройства на основании статистики отказов данного устройства.

Приведённые показатели – это показатели, определяемые по качественным оценкам: мало, нормально, много, отлично, хорошо, удовлетворительно, неудовлетворительно и т.п. Оценка их производится методами неформального оценивания. Примером такого показателя может служить лояльность работника своим руководителям.

Рассмотрим, теперь, механизм оценки информационных рисков. На первом этапе необходимо выяснить, какие угрозы характерны для объекта защиты. Их

принято делить на 3 больших группы: угрозы доступности, целостности и конфиденциальности информации. Каждая из угроз должна принадлежать к одной из групп. Последовательное рассмотрение каждого множества угроз позволит не “пропустить” какую-нибудь из них.

Далее следует рассмотреть уязвимости, через которые может реализоваться угроза. Любая уязвимость актуальна только тогда, когда выполняются три условия – основные факторы. Последовательное рассмотрение каждого основного фактора позволит составить полный перечень косвенных, и “не пропустить” ни одного из них. Оценка показателей косвенных факторов, в свою очередь, позволит принять адекватное решение по нейтрализации угрозы информационной безопасности.

Сложность механизма оценки угроз обусловлена тем, что он не всегда очевиден и может привести к неэффективным или неадекватным решениям. Приведём пример. При работе в электронной информационной базе данных происходит потеря документов из-за частых сбоев в системе электроснабжения (СЭС). Наиболее очевидным решением является установка устройств бесперебойного питания (УБП). Но помогает это не всегда. Допустим, что к одной линии СЭС подключены и компьютеры, и двигатель системы вентиляции помещения. При включении двигателя в линии происходит падение напряжения. Из-за чего и происходит сбой в работе компьютеров. Использование УБП не помогло, так как из-за частых “скачков” напряжения аккумуляторы УБП быстро разряжаются и УБП выходят из строя. Более эффективным будет замена проводов линии электроснабжения на провода с большим сечением или подключение двигателя и компьютеров к разным линиям.

Рассмотрим эту ситуацию в соответствии с изложенной выше методикой. Угрозой безопасности информации является нестабильное электроснабжение. Уязвимости здесь две:

1) недостаточная стабилизация напряжения в СЭС,

2) “слабые” характеристики стабилизации напряжения в блоках питания компьютеров.

Для обоих уязвимостей “на лицо” выполнение всех трёх условий - основных факторов:

1) пространственный фактор – двигатель и компьютеры подключены к одной линии СЭС;

2) временной – двигатель включается и выключается в то же время, когда работают компьютеры;

3) энергетический – в момент включения двигателя – энергии для работы компьютеров не хватает.

Выделим множество параметров:

по первому фактору: необходимость наличия ПК и двигателя на одной линии питания (приведённый показатель: да/нет);

по второму фактору: вероятность одновременной работы двигателя и ПК, рабочее время сотрудников, связанных с работой в базе данных;

по третьему фактору: минимальное напряжение стабильной работы ПК, максимально возможная нагрузка в линии СЭС, сечение проводов линии, вероятность сбоя при включении двигателя.

Рассматривая ситуацию в таком порядке, даже без проведения расчетов, становится очевидным нарушение энергетического фактора – подключение двигателя к другой линии СЭС. Нарушение временного фактора едва ли возможно. Для принятия решения по третьему фактору возможно после проведения расчетов.

3 Требования к выполнению и оформлению контрольной работы

Требования к выполнению и оформлению контрольной работы приведены в документе «Правила оформления письменных работ обучающихся для технических направлений подготовки» ДГТУ, введенные приказами от 16.12.2020 г. № 242.

4 Пример выполнения и оформления контрольной работы

(рамка – это обозначение страницы, её добавлять не надо)

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

Факультет «Информатика и вычислительная техника»

Кафедра «Вычислительные системы и информационная безопасность»

КОНТРОЛЬНАЯ РАБОТА

Дисциплина: «Технологии Web-программирования»

Направление подготовки/специальность: 09.03.02 Информационные системы и технологии

Направленность (профиль): Информационные системы и технологии

Номер зачетной книжки 123456 Номер варианта 10 Группа ВЗИS31

Обучающийся _____ Иван Иванович Иванов
(подпись, дата)

Контрольную работу проверил _____ ст. преподаватель кафедры ВСиИБ, Н.Д. Панасенко
(подпись, дата)

Ростов-на-Дону
2022

Содержание

(необходимо выполнить в соответствии со стандартом ДГТУ оформления контрольных и курсовых работ)

1 Выполнение задания

1.1 Раскрытие темы

Согласно индивидуальному заданию, был создан сайт ресторана.

В процессе работы применялись знания из следующей литературы [1, 2]. (Это ссылка на список перечень использованных информационных ресурсов)

В результате выполнения задания были получены результаты, приведенные на рисунках 1-5.

Рисунок 1 – Результат создания сайта ресторана

Рисунок 2 – Результат создания сайта ресторана

Рисунок 3 – Результат создания сайта ресторана

Рисунок 4 – Результат создания сайта ресторана

5

Рисунок 5 – Результат создания сайта ресторана

Листинг рисунка 1

```
<!DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8">
        <link rel="shortcut icon" href="asico.ico"/>
        <link href="newcss.css" rel="stylesheet" type="text/css"/>
        <title></title>
    </head>
    <body>
        <div class=…
```

…… далее аналогично

Перечень использованных информационных ресурсов

1. Баранов, Р.Д., Иноземцева, С.А. Практические аспекты разработки веб-ресурсов: учебное пособие // Саратов: Вузовское образование, 2018.

2. Техэксперт: официальный сайт сети центров нормативно-технической документации «Техэксперт»: сайт/ АО «Кодекс», 2021. –URL: https://cntd.ru/ (дата обращения: 01.09.2021). – Текст: электронный.

Перечень использованных информационных ресурсов

При изучении дисциплины особое внимание следует обратить на литературные источники согласно таблице 4.

Таблица 4 - Учебно-методическое и информационное обеспечение дисциплины (модуля)

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)				
1. Рекомендуемая литература				
1.1. Основная литература				
	Авторы, составители	Заглавие	Издательство, год	Количество
Л1.1	Смирнов, В.И.	Защита информации: лабораторный практикум	Йошкар-Ола: ПГТУ, 2017	ЭБС
Л1.2	Шаньгин, В.Ф.	Информационная безопасность и защита информации: учебное пособие	Саратов: Профобразование, 2017	ЭБС
Л1.3	Никифоров, С.Н.	Защита информации. Защита от внешних вторжений: учебное пособие	Санкт-Петербург: Санкт-Петербургский государственный	ЭБС
1.2. Дополнительная литература				
Л2.1	Башлы, П. Н., Бабаш, А. В.	Информационная безопасность и защита информации: учебник для студентов вузов	М.: РИОР, 2013	ЭБС
Л2.2	Завгородний, Виктор Иванович	Комплексная защита информации в компьютерных системах: Учеб.пособие для	М.: Логос, 2001	1
Л2.3	Завгородний, В.И.	Комплексная защита информации в компьютерных системах: учеб. пособие	М.: Логос, 2001	6
Л2.4	Деднев, М.А., Дыльнов, Д.В.	Защита информации в банковском деле и электронном бизнесе: [учеб.-справ. изд.]	М.: КУДИЦ-ОБРАЗ, 2004	1
Л2.5	Северин, В.А.	Правовая защита информации в коммерческих организациях: учеб. пособие	М.: Академия, 2009	3
Л2.6	Сергеева, Ю.С.	Защита информации: Конспект лекций; учебное	Москва: А-Приор, 2011	ЭБС
3 Перечень информационных технологий				
3.1 Перечень программного обеспечения				
3.1.1	Microsoft DsktpEdu ALNG LicSAPk OLV E			
3.1.2	Microsoft 0365ProPlusOpenStudents ShrdSvr ALNG SubsVL OLV NL 1Mth Acdmc Stdnt w/Faculty			
3.2 Перечень информационных справочных систем, профессиональные базы данных				
3.2.1	ЭБС «Лань» (https://e.lanbook.com)			
3.2.2	ЭБС «ZNANIUM.COM» (http://znanium.com/)			
3.2.3	ЭБС «РУКОНТ» (http://lib.rucont.ru)			
3.2.4	ЭБС «Университетская библиотека онлайн» (www.biblioclub.ru)			
3.2.5	ЭБС «Юрайт» https://urait.ru/			
3.2.6	ЭБС IPRbooks http://www.iprbookshop.ru/			
3.2.7	Научная электронная библиотека https://elibrary.ru/			
3.2.8	Международная реферативная база данных научных изданий Scopus https://www.scopus.com/			
3.2.9	Международная реферативная база данных научных изданий Web of Science http://www.wokinfo.com/			
3.2.10	Электронная образовательная среда ДГТУ http://skif.donstu.ru/			
3.2.11	Информационно-справочная система «Гарант».			
3.2.12	Информационно-справочная система «Кодекс».			
3.2.13	Информационно-справочная система «Консультант плюс».			
3.2.14	Информационно-справочная система «Техэксперт».			

Содержание