ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Методическое пособие к лабораторным работам и практическим занятиям

2020

Составитель: д-р техн. наук, проф. Ю.М. Краковский

Содержится краткое изложение теоретического материала с указанием списка литературы и контрольных вопросов, а также даны методические рекомендации и варианты шести лабораторных работ.

Приведены лекционные материалы для проведения двух практических занятий.

Рекомендуются студентам и магистрантам различных форм обучения, изучающих дисциплины, связанные с информационной безопасностью информационных систем.

ОГЛАВЛЕНИЕ

Введение

Средства информатизации составляют значительную долю мирового рынка и в существенной мере определяют структуру инвестиционных потоков мирового хозяйства.

Большинство юридических и физических лиц в той или иной мере связаны с такими сферами деятельности, как коммуникация, торговля, финансы, страхование, поэтому рассмотрение вопросов кибербезопасности, защиты информации, анализа информационных рисков является одной из актуальных задач.

Это особенно важно в связи с развитием и внедрением в нашей стране различных сфер цифровой экономики, что, в свою очередь, предъявляет повышенные требования к подготовке специалистов в области информационной безопасности и защиты информации.

Цель защиты системы обработки информации – противодействие угрозам безопасности. Следовательно, безопасная или защищенная система – это система, обладающая средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

Как правило, в системе защиты информации выделяют три обеспечения:

а) правовое, как совокупность законодательных актов и нормативно-правовых документов;

б) организационное, как регламентация деятельности и взаимоотношений исполнителей на нормативно-правовой основе;

в) научно-техническое, как совокупность технических, программно-аппаратных и криптографических методов.

Содержание лабораторных работ и практических занятий ориентировано на первые два обеспечения.

Методическое пособие ориентировано на дисциплины, связанные с безопасностью информационных систем. Оно содержит шесть лабораторных работ и два практических занятия.

Лабораторная работа № 1
«Контроль целостности информации при случайных воздействиях»

Целью работы является изучение сравнение различных методов контроля целостности информации при ее передаче от случайных воздействий.

Введение

В изучаемой дисциплине объектом защиты являются электронные сообщения (документы), поэтому под целостностью будем понимать неискаженность передаваемой, хранимой или обрабатываемой информации.

Целостность информации может быть нарушена путем ее модификации, уничтожения, замены, повтора или другого типа искажения. Целостность информации может нарушиться либо злоумышленником, либо случайным воздействием внешней и внутренней среды, включая людей.

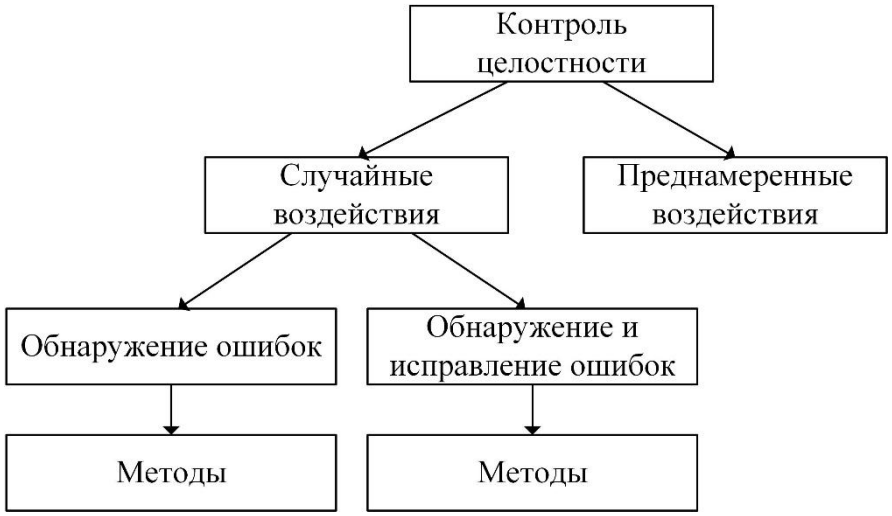

Рис. 1.1. Классификация методов контроля целостности информации

На рисунке 1.1 приведена классификация методов контроля информации по трем факторам:

1) по типу воздействия – а) преднамеренные воздействия, осуществляемые квалифицированным злоумышленником; б) случайные воздействия, которые могут иметь природный характер (стихийные бедствия, магнитные бури), технические причины (аварии, сбои и отказы технических устройств) и человеческий фактор (алгоритмические и программные ошибки разработчиков, ошибки пользователей и обслуживающего персонала);

2) по технологии контроля – а) обнаружение самого факта ошибок без определения их места в сообщении (обнаружение ошибок); б) обнаружения ошибок с определением их побитового места в сообщении и последующего исправления (обнаружение с исправлением ошибок);

3) по числу ошибок (методы) – а) одиночная ошибка; б) более одной ошибки.

В лабораторной работе рассматриваются методы, связанные с обнаружением ошибок. Предполагается, что одна сторона (отправитель) отправляет сообщение, а другая (получатель) получает его. При передаче в канале связи возможно нарушение целостности сообщения от случайных воздействий. Получатель должен иметь возможность проверить нарушена или нет целостность информации.

Нарушение целостности возможно и при хранении, и при обработке сообщений. В этих технологиях также возможно определить «отправителя» и «получателя».

Методы контроля целостности сообщений при обнаружении ошибок

Подчеркнем, что контроль целостности информации при случайных воздействиях охватывает многие этапы ее обработки: обмен информацией между внешней и оперативной памятью, обмен информацией между оперативной памятью и процессором, обработка информации в процессоре, загрузка программ перед их выполнением, передача информации по сетям и т.д.

Опишем общую технологию контроля целостности сообщений при обнаружении ошибок, в которой можно выделить три этапа:

1) отправитель создает сообщение m. Далее, используя выбранный метод контроля, формирует контрольное значение для сообщения – $КО_m$. Полученную пару (m, $КО_m$) передает получателю по каналу связи;

2) получатель, получив эту пару, из сообщения m, используя тот же метод контроля, формирует свое контрольное значение – $КП_m$;

3) далее получатель сравнивает контрольные значения

$$КО_m = КП_m. \qquad (1.1)$$

Если контрольные значения совпадают, то получатель считает, что целостность полученного сообщения не нарушена; иначе она нарушена и надо повторно передать сообщение.

Таким образом, при контроле целостности сообщений методами обнаружения ошибок сравниваются не сами сообщения, а их контрольные значения (1.1).

В случае обнаружения одиночной ошибки на практике используются метод контроля четности и метод контрольной суммы.

При использовании метода контроля четности для каждого байта информации резервируется один разряд (бит), который и является контрольным значением. Значение бита четности является результатом сложения по модулю 2 байта сообщения. Например: 10010010 1; 00010100 0.

Напомним, что таблица истинности для сложения по модулю 2 имеет вид: 0(+)0=0; 1(+)0=1; 0(+)1=1; 1(+)1=0. Отличие от обычного сложения заключается в том, что в последней комбинации при сложении по модулю 2

отсутствует единица переноса, что существенно повышает быстродействие этой операции.

Метод КС

Если сообщение представляется двумерной структурой, то бит четности формируется по каждому столбцу, который является также результатом сложения по модулю 2. Совокупность этих битов четности образует контрольное значение, которое называют контрольной суммой (КС).

Размерность КС определяется размерностью данных в файле. Например: 2, 4, 8-байтовое слово. Рассмотрим пример для 2-байтовых слов:

10010100 01100101
10100010 00011101
<u>10000110 00011101</u>
КС 10110000 01100101

Используя операцию сложения по модулю 2, для первого столбца получим 1, для второго 0 и т.д.

Метод КС используется в сетевых технологиях, например, в протоколе *TCP* для Интернета. При сетевой передаче сообщение разбивается на пакеты, далее для каждого пакета формируется своя КС. Если КС отправителя и получателя совпадают (1.1), то считается, что целостность пакета не нарушена. Иначе требуется повторная передача этого пакета.

Метод КС является достаточно быстродействующим, но он обнаруживает одиночную ошибку по каждому столбцу пакета. Это является недостатком этого метода.

При создании пакетов число слов в нем выбирают таким образом, чтобы вероятностью более одной ошибки можно было пренебречь (она должна быть маленькой). Пакетная передача позволяет достаточно эффективно передавать сообщения даже по не очень надежным каналам.

С учетом недостатка метода КС его в настоящее время стараются не применять. Чтобы контролировать более одной ошибки используют сложение по модулю 2^n, метод циклического контроля и другие методы. Контрольные значения в этих методах также часто называют контрольными суммами.

Рассмотрим сложение по модулю 2^n.

В этом методе осуществляется обычное сложение, а результатом (КС) являются n младших битов. Как правило n равно длине слова в битах: 16, 32, 256, 512 или другая длина.

Рассмотрим сложение четырех чисел, имеющих 4-х битное представление. Эти числа: 14, 15, 11, 13, сумма этих чисел равна 53. В двоичном представлении это будет: 11 0101.

Проведем сложение по модулю 2^4 в двоичном виде:

1110+1111=1 1101+1011=1 1000+1101=1 0101.

Таким образом, КС=0101.

Контроль целостности по модулю 2^n широко используется в криптографии и других методах обработки данных.

Для компактной записи двоичной информации используется шестнадцатеричная система счисления (ШСС). Каждый байт разбивается на две тетрады по четыре бита, эти биты содержат 16 различных чисел ШСС от 0 до 9, а затем от A до F. В таблице 1.1. приведено соответствие между цифрами ШСС и их двоичным 4-х битным представлением (ДСС) от 0000 до 1111.

Таблица 1.1

Таблица соответствия двоичных тетрад и шестнадцатеричных цифр

ДСС	ШСС	ДСС	ШСС	ДСС	ШСС	ДСС	ШСС
0000	0	0100	4	1000	8	1100	C
0001	1	0101	5	1001	9	1101	D
0010	2	0110	6	1010	A	1110	E
0011	3	0111	7	1011	B	1111	F

Например, сообщение FC57D3A6 в двоичном виде будет таким (табл. 1.1): 11111100010101111101001110100110.

Метод CRC

При методе циклического контроля (*CRC*), который позволяет обнаруживать более одной ошибки, сообщение рассматривается как *N*-битное двоичное число, где *N* – количество битов в сообщении. Далее это сообщение делится по модулю 2 на простое целое число до получения остатка. Этот остаток является искомой контрольной суммой.

Делитель должен иметь длину на один бит больше, чем длина КС.

Например, если КС имеет длину 8 бит, то в качестве делителя рекомендуют 100011011 (283) или 101100001 (353), 283 и 353 – это простые числа.

Деление по модулю 2 осуществляется с использованием сложения по модулю 2.

Рассмотрим этот метод на примере (рис. 1.2): сообщение 101111001110, делитель 10011 (19), 19 – это простое число. КС имеет четыре бита:

```
⊕ 101111001110 | 10011
  10011        |
  -----        |
⊕   10010
    10011
    -----
⊕       10111
        10011
        -----
            1000
```

Рис. 1.2. Деление по модулю 2

КС равна 1000, она вычисляется как отправителем, так и получателем.

Помимо применения в локальных сетях, метод *CRC*, например, используется при обмене информацией между оперативной и внешней памятью (винчестером).

Список контрольных вопросов

1. Три аспекта безопасности информации.
2. Что такое конфиденциальность информации.
3. Что такое конфиденциальная информация. Классы конфиденциальности информации.
4. Что такое целостность информации.
5. Что понимается под случайным воздействием на информацию.
6. Опишите технологию контроля информации при случайных воздействиях.
7. Отличие сложения по модулю 2 от обычного сложения.
8. Как осуществляется сложение по модулю 2^n. Привести пример.
9. Сравнить метод КС и метод *CRC*.

Содержание лабораторной работы

1. Используя данные своего варианта (табл. 1.2), записать файл (сообщение m) в виде матрицы, длина строки равна байту, число строк равно четырем. При переходе от 16-ричной системы к двоичной можно использовать таблицу 1.1;
2. Найти контрольную сумму отправителя ($КО_m$);
3. Изменить один бит (выбрать самому) в исходном сообщении и найти контрольную сумму получателя ($КР_m$);
4. Убедиться, что контрольные суммы не совпадают;
5. Изменить два бита в одном столбце исходного сообщения;
6. Найти контрольную сумму получателя ($КР_m$) и убедиться, что контрольные суммы отправителя и получателя совпадают. Объяснить почему;
7. Найти остаток от деления по модулю 2 для исходного сообщения (значение полинома имеется в таблице 1) – (ОО);
8. Найти остаток от деления по модулю 2 для сообщения с двумя ошибками – (ОР);
9. Убедиться, что остатки не совпадают. Объяснить почему.

Оформить лабораторную работу.

Варианты лабораторной работы

Таблица 1.2

№	Исходное сообщение	Полином
1	A6, BC, 67, 9F	100011011
2	C6, BC, D7, 9F	100011011
3	D6, BC, A5, 3A	100011011
4	B4, B1, 6A, 9E	100011011
5	A6, BE, 62, 8C	100011011
6	A7, CC, DA, 9F	100011011
7	B6, AC, 67, 7E	100011011
8	A6, 4C, 52, 9D	100011011
9	CA, B4, D7, 97	101100001
10	D6, BC, A5, 3A	101100001
11	F4, B1, 6A, 9E	101100001
12	C6, BE, 62, 8C	101100001
13	B7, C5, D1, 9F	101100001
14	E3, AC, 6A, 7E	101100001
15	A2, 4C, C2, 9D	101100001
16	A8, BC, E7, 9F	101100001
17	FA, B4, 37, 97	100011011
18	E6, BC, D7, 3A	100011011
19	A4, B1, 6A, 9E	100011011
20	CB, BE, 62, 8C	101100001
21	BF, C8, D1, 9F	101100001
22	ED, AC, 6A, 7E	101100001
23	AB, 4C, C2, 9D	100011011
24	A4, B1, EC, 98	100011011
25	F4, B4, 6A, CE	101100001
26	C6, B9, 62, 9C	101100001
27	B7, CA, D1, AF	101100001
28	E3, A7, 6A, BE	101100001

Лабораторная работа № 2
«Технология обнаружения и исправления ошибок»

Цель работы – освоить технологию обнаружения и исправления ошибок на примере кода Хэмминга.

Введение

Код называется кодом с исправлением ошибок, если всегда из неправильного кодового набора можно получить правильный. Главным для исправления ошибок является то, что необходимо уметь обнаруживать и выделять местоположение ошибочных битов. Если местоположение ошибки определено, то ее исправление производится путем замены ошибочного разряда на его инверсию: 0→1, 1→0.

Код, в котором возможно обнаружить и исправить ошибки, называют помехозащищенным или корректирующим.

Одним из первых корректирующих кодов, для которого одиночная ошибка не только обнаруживается, но и исправляется, является код Хэмминга. Рассмотрим основные принципы его построения.

Код Хэмминга

Пусть сообщение имеет n информативных разрядов ($m1$, ..., mn) и k контрольных разрядов ($p1$, ..., pk), которые используются для контроля целостности сообщения. Пронумеруем позиции каждого из ($n+k$) разрядов расширенного сообщения, начиная со значения 1 для старшего разряда (правый бит) и заканчивая значением ($n+k$) для младшего (левый бит). Контрольные разряды размещаются в позициях с номерами

$$2^{d-1},\ d = 1,2,\ \ldots,\ k,\ (1,\ 2,\ 4,\ \ldots). \qquad (2.1)$$

Отправитель должен сформировать контрольные разряды и вставить их в расширенное сообщение в соответствие с выражением (2.1). Значения контрольных разрядов определяются с использованием сложения по модулю 2 специальных позиций сообщения.

Получатель, используя полученное расширенное сообщение, формирует k-разрядное контрольное слово, используя сложение по модулю 2 специальных позиций расширенного сообщения. Если все разряды этого слова нулевые, то сообщение является целым (принято без искажения).

В любом другом случае код этого слова указывает номер разряда, в котором произошло искажение бита. Получатель, используя операцию инверсии, исправляет ошибку и делает сообщение целым (без искажения). Чтобы в код из k разрядов можно было записать ($n+k+1$) значений, должно выполняться условие

$$2^k \geq n+k+1. \qquad (2.2)$$

Так, например, если n=4, то k=3, а контрольное слово будет иметь восемь значений. Номера контрольных разрядов (2.1): 1, 2, 4; при n=8, учитывая (2.2), k=4, номера контрольных разрядов: 1, 2, 4, 8.

Опишем способ построения кода Хэмминга при n=4 (m1, m2, m3, m4) и k=3 (p1, p2, p3). Для этого приведем перечень комбинаций двоичного кода контрольного слова (c3c2c1) при k=3 (M – десятичное представление двоичного кода) (рис. 2.1):

c3	c2	c1	M	
0	0	0	0	(ошибка отсутствует)
0	0	1	1	
0	1	0	2	
0	1	1	3	
1	0	0	4	
1	0	1	5	
1	1	0	6	
1	1	1	7	

Рис. 2.1. Комбинации контрольного слова

Числа 1–7, представленный на рисунке 2.1, указывают номера ошибочных разрядов в расширенном сообщении:

1	2	3	4	5	6	7
p1	p2	m1	p3	m2	m3	m4

Подгруппы для каждого разряда контрольного слова содержат те номера его комбинаций, которые в данном столбце содержат 1. Например, в столбце для c1 единица присутствует в комбинациях с номерами 1, 3, 5, 7. Исходя из этого, получаются следующие подгруппы:

$$c1 – (\underline{1}, 3, 5, 7); c2 – (\underline{2}, 3, 6, 7); c3 – (\underline{4}, 5, 6, 7). \quad (2.3)$$

Как мы видим, каждый контрольный разряд входит в одну из подгрупп, номера их позиций подчеркнуты. При формировании контрольного слова c3c2c1 к подгруппам (2.3) применяется операция сложения по модулю 2. Напомним, что контрольное слово формирует получатель.

Как мы уже указывали, отправитель формирует контрольные разряды и расставляет их в расширенном сообщении в соответствии с выражением (2.1). При этом он использует следующие подгруппы:

$$p1 – (3, 5, 7); p2 – (3 ,6, 7); p3 – (5, 6, 7). \quad (2.4)$$

Подгруппы (2.4) формируются из подгрупп (2.3).

Если для нашего примера информативная часть расширенного сообщения равна 0101, то с учетом выражения (2.4):

$$p1=0, p2=1, p3=0.$$

Тогда

номера разрядов	1	2	3	4	5	6	7
сообщение			0		1	0	1
отправленное сообщение	0	1	0	0	1	0	1
полученное сообщение	0	1	0	0	1	1	1

Значение контрольного слова (2.3) (используется операция сложения по модулю 2 подгрупп разрядов)

$$c3=1;\ c2=1;\ c1=0;\ (110=6).$$

Таким образом, ошибочен шестой разряд, поэтому единицу в нем надо изменить на ноль (после этого полученное сообщение совпадет с отправленным).

Заметим, что существуют коды, которые обнаруживают и исправляют более одной ошибки. Подобные коды используются в современных процессорах для обнаружения и исправления возможных ошибок при вычислениях.

Список контрольных вопросов

1. Характеристика и классификация угроз информационной безопасности.
2. Дать определение угрозы и уязвимости.
3. Опишите технологию обнаружения и исправления ошибок на примере кода Хэмминга.
4. В чем отличие методов обнаружения ошибок от методов обнаружения и исправления ошибок.
5. Как определить число контрольных разрядов.
6. Как создается контрольное слово и для чего.
7. Сравнить метод КС и метод Хэмминга.

Содержание лабораторной работы

1. Взять первый байт из таблицы 1.2 своего варианта;
2. Получить расширенное сообщение;
3. Получить контрольное слово. Убедиться, что оно состоит из нулей.
4. Изменить один бит (выбрать самому) в расширенном сообщении;
5. Получить контрольное слово и исправить ошибку. Убедиться, что ошибка исправлена правильно.
6. Повторить п. 4 и 5 с другим ошибочным битом.

Оформить лабораторную работу.

Лабораторная работа № 3
«Вероятностный подход к определению длины пароля»

Цель работы – показать связь между атакой в виде перебора паролей и его длиной.

Введение

Идентификация – процедура распознавания пользователя по его идентификатору (имени). Эта функция выполняется, когда пользователь делает попытку войти в систему. Пользователь сообщает системе по ее запросу свой идентификатор, и система проверяет в своей базе данных его наличие.

Аутентификация – процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы: можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После идентификации и аутентификации субъекта выполняется его авторизация.

Авторизация – процедура предоставления субъекту определенных полномочий и ресурсов в данной системе. Иными словами, авторизация устанавливает сферу его действия и доступные ему ресурсы. Если система не может надежно отличить авторизованное лицо от неавторизованного, то конфиденциальность и целостность информации в этой системе могут быть нарушены. Организации необходимо четко определить свои требования к безопасности, чтобы принимать решения о соответствующих границах авторизации.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя.

Администрирование – регистрация действий пользователя в сети, включая его попытки доступа к ресурсам. Хотя эта учетная информация может быть использована для выписывания счета, с позиций безопасности она особенно важна для обнаружения, анализа инцидентов безопасности в сети и соответствующего реагирования на них. Записи в системном журнале и аудиторские проверки – все это может быть использовано для обеспечения подотчетности пользователей, если что-либо случится при входе в сеть с их идентификатором.

Характеристика протоколов аутентификации

Необходимый уровень защиты технологии аутентификации определяется требованиями безопасности, которые установлены в организации. Общедоступные *Web*-серверы могут разрешить анонимный или гостевой доступ к информации. Финансовые транзакции могут потребовать двухфакторной или строгой аутентификации. Надежная аутентификация является тем ключевым фактором, который гарантирует, что только авторизованные пользователи получат доступ к нужной информации.

При защите каналов передачи данных должна выполняться взаимная аутентификация субъектов, т. е. подтверждение подлинности субъектов (отправителя и получателя), связывающихся между собой по линиям связи.

Процедура подтверждения подлинности выполняется обычно в начале сеанса установления соединения абонентов. Термин «соединение» указывает на логическую связь (потенциально двустороннюю) между двумя субъектами сети. Цель данной процедуры – обеспечить уверенность, что соединение установлено с законными субъектами и вся информация дойдет до места назначения.

Для подтверждения своей подлинности субъект может предъявлять системе разные сущности. В зависимости от предъявляемых субъектом сущностей процессы аутентификации могут быть разделены на основе:

а) *знания* чего-либо. Примерами могут служить пароль, персональный идентификационный код *PIN*, а также ключи, знание которых демонстрируется в протоколах типа «запрос – ответ»;

б) *обладания* чем-либо. Примерами могут служить магнитные карты, смарт-карты, токены, сертификаты и другие средства;

в) каких-либо неотъемлемых *характеристик*. Примерами могут служить методы, базирующиеся на проверке биометрических характеристик пользователя – голос, радужная оболочка или сетчатка глаза, отпечатки пальцев, геометрии ладони руки и др.

Пароль – это то, что знает пользователь и другой участник взаимодействия. Для взаимной аутентификации участников может быть организован обмен паролями между ними. При выборе паролей помимо его длины необходимо учитывать, что технологии их восстановления не требует силовой атаки (перебора). Для определения паролей созданы специальные частотные словари, специальные методы, использующие нейронные сети, что упрощает их поиск. Учитывая это, пароли желательно защищать, поэтому их преобразуют при хранении, например, с помощью хэш-функций.

Динамический (одноразовый) пароль – это пароль, который после однократного применения никогда больше не используется. Динамический механизм задания пароля — один из лучших способов защиты процесса аутентификации от угроз извне. Обычно системы аутентификации с одноразовыми паролями используются для проверки удаленных пользователей. Генерация одноразовых паролей может осуществляться аппаратным или программным способом.

Двухфакторная проверка подлинности помогает обеспечить защиту, усложняя вход в вашу учетную запись для другого пользователя. Она использует две различные формы аутентификации: пароль и способ связи, который в данном случае называют сведения безопасности. Даже если кто-то другой узнает ваш пароль, он не сможет войти, если не имеет доступа к сведениям безопасности. При этом необходимо выполнять рекомендацию, связанную с тем, что желательно использовать различные пароли для всех своих учетных записей.

Если включена двухфакторная проверка подлинности, то пользователь для проверки подлинности каждый раз при входе будет получать код безопасности (динамический пароль) по электронной почте, телефону или в приложении.

Основные атаки на протоколы аутентификации:

1) маскарад, когда пользователь выдает себя за другого с целью получения полномочий и возможности действий от лица другого пользователя;

2) подмена стороны аутентификационного обмена, когда злоумышленник в ходе данной атаки участвует в процессе аутентификационного обмена между двумя сторонами с целью модификации проходящего через него трафика;

3) повторная передача, которая заключается в повторной передаче аутентификационных данных каким-либо пользователем;

4) принудительная задержка, когда злоумышленник перехватывает некоторую информацию и передает ее спустя некоторое время;

5) перехват, когда злоумышленник перехватывает аутентификационный трафик и пытается получить информацию о долговременных криптографических ключах.

Вероятностный подход к определению длины пароля

Рассмотрим вероятностный подход к определению длины пароля, когда используется атака в виде перебора паролей. С какой-то вероятностью пароль может быть угадан.

Введем такие обозначения:

n – число различных символов, которые можно использовать при создании пароля (мощность алфавита);

N – число возможных паролей;

v – скорость подбора паролей, паролей/сек;

T – время действия пароля, сутки;

u – необходимая длина пароля по числу символов.

Длина пароля должна обеспечивать вероятность его угадывания (p) меньше заданного значения этой вероятности: $p < p_z$.

Вероятность подбора (угадывания) пароля и число возможных паролей равны

$$p < p_z = 86400 \cdot v \cdot T/N,\ N = n^u, \qquad (3.1)$$

где 86400 – число секунд в сутках.

Замечание: рассматриваются все возможные варианты паролей, хотя на практике это не всегда выполняется.

С учетом (3.1), необходимая длина пароля

$$u > \lg(86400 \cdot v \cdot T/p_z)/\lg(n). \qquad (3.2)$$

Возьмем как пример такие исходные данные: $p_z=10^{-4}$; $v=10^4$ паролей/сек; T=10 суток.

Виды символов: большие и маленькие русские и английские буквы, цифры (n=128).

Учитывая (3.2) и исходные данные: $u > 6{,}6 = 7$.

Пароль должен иметь не менее 7 разнообразных символа (в примере символы могут повторяться). Примерами такого пароля являются:

Ва12*Sdf*; *hGJ*13ро; КуЦ78*BN*.

Список контрольных вопросов

1. В чем заключаются преимущества и недостатки парольной технологии аутентификации.
2. Что такое процедура аутентификации. Как она связана с процедурой идентификации.
3. Двухфакторная проверка подлинности.
4. Основные атаки на протоколы аутентификации.
5. Дать характеристику стандартов безопасности информационный технологий.

Содержание лабораторной работы

1. Используя исходные данные по своему варианту (табл. 3.1), определить длину пароля для трех случаев заданного значения вероятности: p_z.
2. Для каждого полученного значения длины пароля предложить три его варианта.
3. Оформить лабораторную работу.

Замечание: во всех вариантах в качестве символов используются большие и маленькие русские и английские буквы, а также цифры (n=128).

Варианты лабораторной работы

Таблица 3.1

№	v	T	p_z
1	$v=10^4$	12	10^{-4}, 10^{-5}, 10^{-6}
2	$v=5\cdot 10^4$	10	10^{-4}, 10^{-5}, 10^{-6}
3	$v=8\cdot 10^4$	11	10^{-4}, 10^{-5}, 10^{-6}
4	$v=7\cdot 10^4$	13	10^{-4}, 10^{-5}, 10^{-6}
5	$v=4\cdot 10^4$	14	10^{-4}, 10^{-5}, 10^{-6}
6	$v=10^5$	12	10^{-4}, 10^{-5}, 10^{-6}
7	$v=5\cdot 10^5$	10	10^{-4}, 10^{-5}, 10^{-6}
8	$v=8\cdot 10^5$	11	10^{-4}, 10^{-5}, 10^{-6}
9	$v=7\cdot 10^5$	13	10^{-4}, 10^{-5}, 10^{-6}
10	$v=3\cdot 10^5$	14	10^{-4}, 10^{-5}, 10^{-6}
11	$v=10^4$	11	10^{-4}, 10^{-5}, 10^{-6}
12	$v=5\cdot 10^4$	12	10^{-4}, 10^{-5}, 10^{-6}
13	$v=8\cdot 10^4$	15	10^{-4}, 10^{-5}, 10^{-6}
14	$v=7\cdot 10^4$	10	10^{-4}, 10^{-5}, 10^{-6}
15	$v=4\cdot 10^4$	13	10^{-4}, 10^{-5}, 10^{-6}
16	$v=10^5$	11	10^{-4}, 10^{-5}, 10^{-6}
17	$v=5\cdot 10^5$	12	10^{-4}, 10^{-5}, 10^{-6}
18	$v=8\cdot 10^5$	15	10^{-4}, 10^{-5}, 10^{-6}
19	$v=7\cdot 10^5$	10	10^{-4}, 10^{-5}, 10^{-6}
20	$v=3\cdot 10^5$	13	10^{-4}, 10^{-5}, 10^{-6}
21	$v=5\cdot 10^5$	12	10^{-4}, 10^{-5}, 10^{-6}
22	$v=8\cdot 10^5$	10	10^{-4}, 10^{-5}, 10^{-6}
23	$v=7\cdot 10^5$	11	10^{-4}, 10^{-5}, 10^{-6}
24	$v=3\cdot 10^5$	13	10^{-4}, 10^{-5}, 10^{-6}
25	$v=10^4$	14	10^{-4}, 10^{-5}, 10^{-6}
26	$v=5\cdot 10^4$	10	10^{-4}, 10^{-5}, 10^{-6}
27	$v=8\cdot 10^4$	13	10^{-4}, 10^{-5}, 10^{-6}
28	$v=3\cdot 10^5$	11	10^{-4}, 10^{-5}, 10^{-6}

Лабораторная работа № 4
«Методика определения информационных рисков»

Цель работы – освоить технологию оценки информационного риска по трехфакторной модели.

Введение

Под информационным риском понимают средние ожидаемые потери объекта защиты от реализации угрозы при существовании и использовании уязвимости в системе защиты информации. Таким образом, информационный риск оценивает средний размер ущерба, который может быть нанесен в результате некоторого сложного негативного события.

Методика определения информационных рисков базируется на трехфакторной модели

$$R=P_{уг}\cdot P_{уз}\cdot C_{п}, \qquad (4.1)$$

где R – значение (уровень) информационного риска; $P_{уг}$ – вероятность появления угрозы; $P_{уз}$ – вероятность использования уязвимости системы защиты информации; $C_{п}$ – потери от свершившегося происшествия.

При управлении рисками определяются угрозы, уязвимости, оценивается возможный ущерб и вырабатываются контрмеры.

Оценка рисков осуществляется до и после внедрения контрмер.

Если рассматриваемые факторы оцениваются количественно, то говорят о значении риска (количественное измерение размера ущерба). Если эти факторы оцениваются качественно на основании информации экспертов, то речь идет об уровне информационного риска. В лабораторной работе рассматривается второй подход.

Лабораторная работа состоит из двух частей.

В первой части работы экспертно создается таблица для определения уровня информационного риска от выделенных трех факторов.

Во второй части работы определяется уровень информационного риска конкретной анализируемой ситуации.

Создание таблицы для определения уровня информационного риска от трех факторов

Рассмотрим первую часть лабораторной работы (моделирует работу экспертов). Все три фактора, входящих в формулу (4.1), оцениваются специалистами, ответственными за информационную безопасность в организации. При этом они используют шкалы, которые подготавливают эксперты по всем трем факторам и по информационному риску. В общем случае шкала характеризуется числом уровней, наименованием уровней, а также экспертным описанием каждого уровня или специальной таблицей.

В лабораторной работе для вероятностей $P_{уг}$ и $P_{уз}$ используется три шкалы (наименования уровней заглавные русские буквы):

ШР3 (3 уровня): низкий (Н), средний (С), высокий (В);

ШР4 (4 уровня): низкий (Н), средний (С), высокий (В), очень высокий (ОВ);

ШР5 (5 уровней): очень низкий (ОН), низкий (Н), средний (С), высокий (В), очень высокий (ОВ).

При этом для вероятности угрозы используются шкалы ШР3 и ШР4, а для вероятности уязвимости используются шкалы ШР4 и ШР5.

Выбор уровней специалистами осуществляются по таблицам, которые устанавливают соответствие между баллами и уровнями. Эти таблицы готовят эксперты.

Для оценки потерь ($C_{\text{п}}$) используется одна 5-и уровневая шкала (ШС5) (необходимо обратить внимание на экспертное описание уровней):

– *N* (*Negligible*) – очень незначительные потери: воздействием можно пренебречь;

– *Mi* (*Minor*) - незначительные потери: последствия легко устранимы, затраты на ликвидацию последствий невелики, воздействие на информационную технологию незначительно;

– *Mo* (*Moderate*) - происшествие с умеренными потерями: ликвидация последствий не связана с крупными затратами, воздействие на информационную технологию небольшое и не затрагивает критически важные задачи;

– *S* (*Serious*) - происшествие с серьезными потерями: ликвидация последствий связана со значительными затратами, воздействие на информационные технологии ощутимо, влияет на выполнение критически важных задач;

– *C* (*Critical*) - происшествие с очень серьезными потерями: происшествие приводит к невозможности решения критически важных задач.

Для информационного риска используется три шкалы (наименования уровней заглавные русские буквы):

- ШR3 (3 уровня): низкий риск (НР), средний риск (СР), высокий риск (ВР);

- ШR4 (4 уровня): низкий риск (НР), средний риск (СР), высокий риск (ВР), очень высокий риск (ОВР);

- ШR5 (5 уровней): очень низкий риск (ОНР), низкий риск (НР), средний риск (СР), высокий риск (ВР), очень высокий риск (ОВР).

Необходимо построить таблицу для определения уровня информационного риска от трех факторов. Таких таблиц получается четыре в зависимости от уровней вероятностей ($P_{\text{уг}}$, $P_{\text{уз}}$):

(3, 3), (3, 4), (4, 4), 4, 5).

Число строк в этой таблице зависит от числа уровней вероятностей ($P_{\text{уг}}$, $P_{\text{уз}}$):

а) (3, 3) – 9 строк; (3, 4) – 12 строк; (4, 4) – 16 строк; (4, 5) – 20 строк.

Число столбцов этой таблицы зависит от числа уровней шкалы потерь (ШС5), в нашем случае 5 столбцов. Для примера приведена таблица для уровней (3, 3) (табл. 4.1).

Заполнение таблицы 4.1 зависит от числа уровней риска. Это заполнение выполняет студент, исходя из своего варианта. Приведем пример ее заполнения для 3-х уровневого риска (табл. 4.2).

Таблица 4.1

Таблица для заполнения уровней риска

Уровень для $P_{УГ}$	Уровень для $P_{УЗ}$	Уровни шкалы потерь (ШС5)				
		N	*Mi*	*Mo*	*S*	*C*
Н	Н					
	С					
	В					
С	Н					
	С					
	В					
В	Н					
	С					
	В					

Таблица 4.2

Таблица для определения уровня риска

Уровень для $P_{УГ}$	Уровень для $P_{УЗ}$	Уровни шкалы потерь (ШС5)				
		N	*Mi*	*Mo*	*S*	*C*
Н	Н	НР	НР	НР	СР	СР
	С	НР	НР	СР	СР	ВР
	В	НР	СР	СР	ВР	ВР
С	Н	НР	НР	СР	СР	ВР
	С	НР	НР	СР	СР	ВР
	В	НР	СР	ВР	ВР	ВР
В	Н	НР	НР	СР	СР	ВР
	С	НР	СР	ВР	ВР	ВР
	В	СР	СР	ВР	ВР	ВР

После создания таблицы 4.2 первая часть лабораторной работы заканчивается.

Определение уровня информационного риска конкретной ситуации

Рассмотрим вторую часть лабораторной работы.

При определении уровня информационного риска для конкретной ситуации, необходимо оценить вероятности угроз и уязвимостей в зависимости от влияющих факторов. Для этого по угрозам и уязвимостям выделяются косвенные факторы, по которым предлагаются вопросы и несколько фиксированных вариантов ответов, которые «стоят» определенное количество баллов. Итоговая оценка угрозы и уязвимости данного класса определяется путем суммирования баллов.

Далее по таблице соответствия определяется уровень вероятностей угрозы и уязвимости. В варианте лабораторной работы студенту даны суммарные баллы для вероятностей угрозы (Б_$Р_{уг}$) и уязвимости (Б_$Р_{уз}$).

В таблице 4.3 приведено соответствие между значением Б_$Р_{уг}$ и уровнем вероятности угрозы (У_$Р_{уг}$), а в таблице 4.4 приведено соответствие между значением Б_$Р_{уз}$ и уровнем вероятности уязвимости (У_$Р_{уз}$).

Таблица 4.3

Определение уровней для вероятности угрозы

Балл для $P_{уг}$	Уровень для $P_{уг}$	Балл для $P_{уг}$	Уровень для $P_{уг}$
Б_$Р_{уг} \le 12$	Н	Б_$Р_{уг} \le 15$	Н
$12 <$ Б_$Р_{уг} \le 24$	С	$15 <$ Б_$Р_{уг} \le 32$	С
$24 <$ Б_$Р_{уг} \le 36$	В	Б_$Р_{уг} > 32$	В
Б_$Р_{уг} > 36$	ОВ	-	-

Таблица 4.4

Определение уровней для вероятности уязвимости

Балл для $P_{уз}$	Уровень для $P_{уз}$	Балл для $P_{уз}$	Уровень для $P_{уз}$
Б_$Р_{уз} \le 7$	ОН	Б_$Р_{уз} \le 10$	Н
$7 <$ Б_$Р_{уз} \le 16$	Н	$10 <$ Б_$Р_{уз} \le 21$	С
$16 <$ Б_$Р_{уз} \le 25$	С	$21 <$ Б_$Р_{уз} \le 32$	В
$25 <$ Б_$Р_{уз} \le 34$	В	Б_$Р_{уз} > 32$	ОВ
Б_$Р_{уз} > 34$	ОВ	-	-

Содержание лабораторной работы

Исходные данные по варианту лабораторной работы необходимо взять из таблицы 4.5.

1. Ввести последовательно исходные данные для своего варианта.

2. Исходя из числа уровней вероятности угрозы, необходимо ввести их наименования (шкалы ШР3 или ШР4).

3. Исходя из числа уровней вероятности уязвимости, необходимо ввести их наименования (шкалы ШР4 или ШР5).

4. Исходя из числа уровней риска, необходимо ввести их наименования (шкалы ШR3, ШR4 или ШR5).

5. Если наименования уровней вероятностей введены верно, то на экране появляется таблица 4.1.

6. Далее необходимо сформировать таблицу 4.2. Это осуществляется заполнением таблицы 4.1 уровнями информационного риска.

Созданием таблицы 4.2 завершается первый этап лабораторной работы.

7. Исходя из значения балла для вероятности угрозы и числа ее уровней, по таблице 4.3 определяется значение уровня этой вероятности – $У\_Р_{уг}$. Этот уровень вводится, а затем проверяется.

8. Исходя из значения балла для вероятности уязвимости и числа ее уровней, по таблице 4.4 определяется значение уровня этой вероятности – $У\_Р_{уз}$. Этот уровень вводится, а затем проверяется.

9. Исходя из значения уровня для потерь и полученных уровней для вероятностей ($У\_Р_{уг}$ и $У\_Р_{уз}$), по таблице 4.2 определяется уровень риска исследуемой ситуации. Этот уровень вводится, а затем проверяется.

10. Полученный уровень информационного риска является завершением второго этапа и лабораторной работы в целом.

11. Перейти к защите лабораторной работы.

Список контрольных вопросов

1. Как оценить вероятность негативного случайного события.
2. Основные стандарты управления информационной безопасности.
3. Методы оценки субъективных вероятностей.
4. Управление рисками информационной безопасности.
5. Понятие уязвимости системы защиты информации.
6. Возможные подходы к оценке рисков.
7. Этапы процесса управления рисками.
8. Назначение и функции программных продуктов для управления информационной безопасности, включая комплекс КОНДОР+2.2.
9. Анализ и контроль рисков с помощью системы ГРИФ.
10. Вопросы по методике определения информационных рисков.

Варианты лабораторной работы

Таблица 4.5

№ варианта	Число уровней риска R	Число уровней для $P_{уг}$	Число уровней для $P_{уз}$	Балл для $P_{уг}$ (Б_$P_{уг}$)	Балл для $P_{уз}$ (Б_$P_{уз}$)	Уровень для потерь
1	5	4	4	15	27	*Mi*
2	5	3	4	27	18	*Mo*
3	5	4	5	8	32	*C*
4	4	4	4	43	28	*S*
5	4	3	4	38	24	*N*
6	4	4	5	19	14	*Mo*
7	5	4	4	27	18	*Mo*
8	5	3	4	15	24	*Mi*
9	5	4	5	8	32	*S*
10	4	4	4	43	28	*C*
11	4	3	4	38	24	*Mo*
12	4	4	5	19	14	*Mi*
13	3	4	4	16	19	*N*
14	3	4	5	32	29	*C*
15	3	4	4	16	19	*Mi*
16	3	4	5	32	29	*S*
17	5	4	5	25	22	*C*
18	5	4	4	17	28	*S*
19	5	4	5	18	22	*S*
20	4	4	4	33	38	*C*
21	4	3	4	28	14	*N*
22	4	4	5	29	24	*Mo*
23	4	3	5	43	28	*S*
24	4	3	5	38	24	*N*
25	4	4	4	19	14	*Mo*
26	5	4	4	27	18	*Mo*
27	5	3	4	15	24	*Mi*
28	5	3	4	27	18	*Mo*

Лабораторная работа № 5
«Порядок проведения классификация информационных систем в РФ»

Цель работы – освоить порядок проведения классификации информационных систем в соответствии с требованиями Приказа ФСТЭК России от 11 февраля 2013 г. №17 с учетом приказа ФСТЭК от 15.02.2017 г. № 27.

Введение

В последнее десятилетие в Российской Федерации государственными регуляторами активно проводятся мероприятия по совершенствованию организационно-правовой базы в сфере защиты информационных систем различного назначения. Можно отметить следующие значимые документы, которые появились в это время:

– приказ ФСТЭК России_ «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11.02.2013 № 17;

– приказ ФСТЭК России_«Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» от 14.03.2014 № 31.

– приказ ФСТЭК от 15.02.2017 г. № 27 в развитие приказа ФСТЭК от 11.02.2013 № 17;

– приказ ФСТЭК от 27.03.2017 г. № 49 в развитие приказа ФСТЭК от 14.03.2014 № 31.

Приказ № 17 с учетом приказа № 27 для защиты государственных ИС предусматривает проведение следующих мероприятий:

– принятие решения о необходимости защиты информации в ИС;

– классификацию ИС по требованиям защиты информации;

– определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации;

– определение требований к системе защиты информации информационной системы.

Приказ №17 с учетом приказа № 27 устанавливает обязательные требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней при обработке указан-

ной информации в государственных и муниципальных информационных системах (ИС).

В документах не рассматриваются требования о защите информации, связанные с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации.

Требования к системе защиты информации ИС определяются в зависимости от:

1) класса защищенности ИС;

2) угроз безопасности информации, включенных в модель угроз безопасности информации.

Базовый набор мер защиты информации

Состав базового набора мер защиты информации для установленного класса защищенности ИС определены приложением к приказу № 27.

Учитывая важность этого приложения, оно приведено в приложении № 1 данного методического пособия.

Эти меры содержат 13 разделов.

Расширенный набор мер защиты информации в государственных ИС, не содержащих государственную тайну, определен методическим документом ФСТЭК РФ от 11.02.2014 г.

В соответствие с этим документом выбор мер защиты информации для их реализации в государственных ИС в рамках ее системы защиты информации включает следующие этапы:

– определение базового набора мер защиты информации для установленного класса защищенности ИС в соответствии с базовыми наборами мер защиты информации, разработанных ФСТЭК;

– адаптация базового набора мер защиты информации применительно к структурно-функциональным характеристикам ИС, информационным технологиям, особенностям функционирования ИС (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с информационными технологиями, не используемыми в ИС, или структурно-функциональными характеристиками, не свойственными ИС);

– уточнение адаптированного базового набора мер защиты информации с учетом, не выбранных ранее мер защиты информации в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в модель угроз безопасности информации;

– дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации.

В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации

(bdu.fstec.ru), а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации.

В целом для обеспечения защиты информации, содержащейся в ИС, проводятся следующие мероприятия:

– формирование требований к защите информации, содержащейся в ИС (зависит от определенного в итоге набора мер защиты информации в ИС);

– разработка системы защиты информации ИС (определение организационных мероприятий, выбор технических и физических средств защиты информации в том числе для реализации определенного набора мер защиты);

– внедрение системы защиты информации ИС;

– аттестация информационной системы по требованиям защиты информации (проводится лицензиатами ФСТЭК России) и ввод ее в действие;

– обеспечение защиты информации в ходе эксплуатации аттестованной ИС;

– обеспечение защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации.

Определение класса защищенности ИС

Определение класса защищенности ИС является обязательным этапом при определении мер защиты информации.

Приказ ФСТЭК № 27 совместно с приказом № 17 устанавливает обязательные требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней при обработке указанной информации в государственных и муниципальных ИС.

В документах не рассматриваются требования о защите информации, связанные с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации.

Если при описании назначения ИС было выделено несколько видов информации (служебная тайна, налоговая тайна и иные установленные законодательством Российской Федерации виды информации ограниченного доступа), то определяется итоговый уровень значимости информации;

Приказ № 27 устанавливает три класса защищённости ИС:

– первый класс (К1) (наивысший с точки зрения защиты);

– второй класс (К2);

– третий класс (К3).

Класс защищенности (КЗ) ИС определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой ИС, и масштаба информационной системы (М)

$$КЗ(УЗ, М). \qquad (5.1)$$

Уровень значимости информации, обрабатываемой в ИС, зависит от трех факторов, связанных с аспектами безопасности информации:

– степень возможного ущерба от нарушения конфиденциальности информации в ИС (неправомерный доступ, копирование, предоставление или распространение) (СВУ_К);

– степень возможного ущерба от нарушения целостности информации в ИС (неправомерные уничтожение или модифицирование) (СВУ_Ц);

– степень возможного ущерба от нарушения доступности (неправомерное блокирование) информации в ИС (СВУ_Д);

$$УЗ(СВУ\_К, СВУ\_Ц, СВУ\_Д). \quad (5.2)$$

Каждый этот фактор зависит от степени возможного ущерба ИС и имеет три уровня, которые определяются по созданной экспертами 3-х уровневой шкале:

– высокий (В), если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) ИС и (или) организация не могут выполнять возложенные на них функции;

– средний (С), если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) ИС и (или) организация не могут выполнять хотя бы одну из возложенных на них функций;

– низкий (Н), если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) ИС и (или) организация могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

Уровень значимости информации определяется по 3-х входовой таблице 5.1, которая реализует модель (5.2).

Информация имеет высокий уровень значимости (УЗ=УЗ1), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба.

Информация имеет средний уровень значимости (УЗ=УЗ2), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба.

Таблица 5.1

Определение уровня значимости информации

СВУ_К																										
В									С									Н								
СВУ_Ц									СВУ_Ц									СВУ_Ц								
В			С			Н			В			С			Н			В			С			Н		
СВУ_Д			СВУ_Д			СВУ_Д			СВУ_Д			СВУ_Д			СВУ_Д			СВУ_Д			СВУ_Д			СВУ_Д		
В	С	Н	В	С	Н	В	С	Н	В	С	Н	В	С	Н	В	С	Н	В	С	Н	В	С	Н	В	С	Н
1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	1	2	2	1	1	1	1	2	2	1	2	3

Информация имеет минимальный уровень значимости (УЗ=УЗ3), если степень ущерба от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности) имеют минимальный уровень (Н).

Например, если СВУ_К=С, СВУ_Ц=В, а СВУ_Д=Н, то УЗ=УЗ1.

При обработке в ИС двух и более видов информации (служебная тайна, налоговая тайна и иные установленные законодательством Российской Федерации виды информации ограниченного доступа), уровень значимости информации определятся отдельно для каждого вида информации. Итоговый уровень значимости информации, обрабатываемой в ИС, устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности и доступности информации каждого вида информации.

Масштаб (М) ИС может иметь три уровня и определяется по созданной экспертами 3-х уровневой шкале:

– федеральный масштаб (Ф), если она функционирует на территории Российской Федерации (в пределах федерального округа) и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях;

– региональный масштаб (Р), если она функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях;

– объектовый масштаб (О), если она функционирует на объектах одного федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

Класс защищенности (КЗ) ИС определяется по 2-х входовой таблице 5.2, которая реализует модель (5.1).

Например, если УЗ=УЗ1, а М=Р, то КЗ=1.

Еще раз подчеркнем, класс защищенности ИС влияет на базовый набор мер защиты. Этот базовый набор определен приложением к приказу № 27 по 13 разделам, приведенном в приложении № 1 к лабораторной работе.

.

Таблица 5.2

Определение класса защищенности ИС

УЗ	М		
	Ф	Р	О
УЗ1	КЗ=1	КЗ=1	КЗ=1
УЗ2	КЗ=1	КЗ=2	КЗ=2
УЗ3	КЗ=2	КЗ=3	КЗ=3

Меры защиты информации, не обозначенные знаком «+», применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер защиты информации в информационной системе соответствующего класса защищенности.

Последовательность определения класса защищенности ИС

Таким образом, в соответствии с приказом №17 с учетом приказа ФСТЭК от 15.02.2017 г. № 27 класс защищенности ИС определяется в такой последовательности:

1) Описывается назначение и особенности ИС (таблица 5.3). Если какие-то аспекты безопасности не выделяются, то они имеют низкий уровень (Н);

2) Исходя из полученного описания, определяются: а) уровни степени возможного ущерба для факторов (5.2) (В, С, Н); б) уровень масштаба (Ф, Р, О);

3) Используя таблицу 5.1, определяют уровень значимости информации (1, 2, 3);

4) Если при описании назначения ИС было выделено несколько видов информации (служебная тайна, налоговая тайна и иные установленные законодательством Российской Федерации виды информации ограниченного доступа), то определяется итоговый уровень значимости информации;

5) Используя таблицу 5.2, определяют класс защищенности ИС.

Содержание лабораторной работы, соответствует последовательности определения класса защищенности ИС

Исходное описание ИС по варианту лабораторной работы необходимо взять из таблицы 5.3.

1. Исходя из своего варианта, определить исходные данные.
2. Определить итоговый уровень значимости информации (УЗ) для ИС;

3. Определить класс защищённости ИС (КЗ), что является завершением лабораторной работы.

Оформить лабораторную работу.

Список контрольных вопросов

1. Правовое обеспечение информационной безопасности.
2. Организационное обеспечение информационной безопасности.
3. Функции органов государственной власти, обеспечивающих информационную безопасность в Российской Федерации.
4. Основные функции ФСТЭК.
5. Особенности обработки персональных данных.
6. Сфера применимости Приказа №17.
7. Виды ИС по масштабу.
8. На основании каких данных формируются требования к системе защиты информации ИС.
9. Перечень мероприятий для обеспечения защиты информации, содержащейся в ИС.
10. Порядок классификации ИС.
11. Вопросы по классификации ИС.

Варианты лабораторной работы

Таблица 5.3

№	Описание ИС
1	ИС функционирует в 3 федеральных округах РФ; содержит сведения, составляющие банковскую тайну. ИС предназначена для обеспечения деятельности большого банка; нарушение конфиденциальности влечет существенные последствия для организации.
2	ИС функционирует в пределах одного федерального округа РФ; содержит сведения, составляющие налоговую тайну; нарушение целостности информации влечет умеренные последствия; нарушение конфиденциальности влечет существенные последствия.
3	ИС функционирует в одном федеральном округе РФ, но в нескольких субъектах РФ. Содержит сведения, составляющие врачебную тайну. Нарушение конфиденциальности и доступности влечет существенные последствия для организации.
4	ИС функционирует в одном федеральном округе РФ, но в нескольких субъектах РФ. Содержит сведения, составляющие нотариальную тайну. Нарушение доступности и целостности влечет существенные последствия для организации.
5	ИС функционирует в 5 субъектах РФ. Содержит сведения, составля-

	ющие тайну следствия. Нарушение конфиденциальности и целостности влечет существенные последствия для организации.
6	ИС функционирует в 5 субъектах РФ. Содержит сведения, составляющие коммерческую тайну. Нарушение конфиденциальности и целостности влечет умеренные последствия для организации.
7	ИС функционирует в одной организации РФ. Содержит конфиденциальные сведения, предназначенные для управления технологически опасными процессами. Нарушение конфиденциальности, целостности и доступности влечет существенные последствия для организации.
8	ИС функционирует в одной организации РФ. Содержит конфиденциальные сведения, предназначенные для экономической деятельности. Нарушение конфиденциальности и доступности влечет существенные последствия для организации; нарушение целостности информации влечет умеренные последствия.
9	ИС функционирует в пределах одного федерального округа РФ. Содержит конфиденциальные сведения, предназначенные для принятия управленческих решений. Нарушение конфиденциальности и доступности влечет умеренные последствия для организации, а нарушение целостности - существенные.
10	ИС функционирует в одной организации. Содержит конфиденциальные сведения, предназначенные для управления технологически опасными процессами. Нарушение целостности и доступности влечет существенные последствия для организации.
11	ИС охватывает семь муниципальных образований РФ. Содержит сведения, составляющие адвокатскую тайну. Нарушение целостности и доступности влечет умеренные последствия для организации, а нарушение конфиденциальности - существенные.
12	ИС охватывает семь муниципальных образований РФ. Содержит сведения, составляющие врачебную тайну. Нарушение целостности и конфиденциальности влечет существенные последствия для организации.
13	ИС функционирует в одной организации. Содержит конфиденциальные сведения, предназначенные для экономической деятельности. Нарушение конфиденциальности и доступности влечет умеренные последствия для организации, а нарушение целостности - существенные последствия.
14	ИС функционирует в одной организации. Содержит конфиденциальные сведения, предназначенные для госуправления. Нарушение целостности и конфиденциальности влечет умеренные последствия для организации.
15	ИС функционирует в одной организации. Содержит конфиденциальную информацию (персональные данные). Последствия для организации от нарушения целостности, доступности и конфиденциально-

	сти информации имеют умеренные значения.
16	ИС охватывает шесть муниципальных образований РФ. Содержит конфиденциальную информацию (персональные данные). Нарушение целостности и конфиденциальности влечет существенные последствия для организации.
17	ИС функционирует в трех субъектах РФ. Содержит сведения, составляющие врачебную тайну. Нарушение конфиденциальности влечет умеренные последствия для организации, а нарушение целостности влечет существенные последствия.
18	ИС функционирует в трех субъектах РФ. Содержит сведения, составляющие коммерческую тайну. Нарушение конфиденциальности и доступности влечет умеренные последствия для организации.
19	ИС функционирует в одной организации. Содержит конфиденциальные сведения, предназначенные для принятия управленческих решений. Последствия для организации от нарушения целостности и конфиденциальности информации умеренные, а нарушение доступности влечет существенные последствия.
20	ИС функционирует в одной организации. Содержит конфиденциальные сведения, предназначенные для экономической отчетности. Последствия для организации от нарушения целостности, доступности и конфиденциальности информации не определены.
21	ИС охватывает семь муниципальных образований РФ. Содержит сведения, составляющие адвокатскую тайну. Нарушение целостности и доступности влечет умеренные последствия для организации, а нарушение конфиденциальности - существенные.
22	ИС охватывает семь муниципальных образований РФ. Содержит сведения, составляющие врачебную тайну. Нарушение целостности и конфиденциальности влечет существенные последствия для организации.
23	ИС функционирует в одной организации. Содержит конфиденциальные сведения, предназначенные для экономической деятельности. Нарушение конфиденциальности и доступности влечет умеренные последствия для организации, а нарушение целостности - существенные последствия.
24	ИС функционирует в одной организации. Содержит конфиденциальные сведения, предназначенные для госуправления. Нарушение целостности и конфиденциальности влечет умеренные последствия для организации.
25	ИС функционирует в одной организации. Содержит конфиденциальную информацию (персональные данные). Последствия для организации от нарушения целостности, доступности и конфиденциальности информации имеют умеренные значения.
26	ИС охватывает шесть муниципальных образований РФ. Содержит конфиденциальную информацию (персональные данные). Нарушение

	целостности и конфиденциальности влечет существенные последствия для организации.
27	ИС функционирует в трех субъектах РФ. Содержит сведения, составляющие врачебную тайну. Нарушение конфиденциальности влечет умеренные последствия для организации, а нарушение целостности влечет существенные последствия.
28	ИС функционирует в трех субъектах РФ. Содержит сведения, составляющие коммерческую тайну. Нарушение конфиденциальности и доступности влечет умеренные последствия для организации.

Студент должен оформить лабораторную работу в соответствии с заданием и защитить.

ПРИЛОЖЕНИЕ 1

СОСТАВ
МЕР ЗАЩИТЫ ИНФОРМАЦИИ И ИХ БАЗОВЫЕ НАБОРЫ
ДЛЯ СООТВЕТСТВУЮЩЕГО КЛАССА ЗАЩИЩЕННОСТИ
ИНФОРМАЦИОННОЙ СИСТЕМЫ

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Классы защищенности информационной системы		
		3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)				
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных		+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+
ИАФ.7	Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами дан-			

	ных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа			
II. Управление доступом субъектов доступа к объектам доступа (УПД)				
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+	+	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации			
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему			
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы			+
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	+	+	+
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информаци-			

	ей в процессе ее хранения и обработки			
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники		+	+
III. Ограничение программной среды (ОПС)				
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения			+
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения		+	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	+	+	+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов			
IV. Защита машинных носителей информации (ЗНИ)				
ЗНИ.1	Учет машинных носителей информации	+	+	+
ЗНИ.2	Управление доступом к машинным носителям информации	+	+	+
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны			
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах			

ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации		+	+
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации			
ЗНИ.7	Контроль подключения машинных носителей информации			
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	+	+	+
V. Регистрация событий безопасности (РСБ)				
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти	+	+	+
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	+	+	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	+	+	+
РСБ.7	Защита информации о событиях безопасности	+	+	+
РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе			
VI. Антивирусная защита (АВЗ)				
АВЗ.1	Реализация антивирусной защиты	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+
VII. Обнаружение вторжений (СОВ)				
СОВ.1	Обнаружение вторжений		+	+
СОВ.2	Обновление базы решающих правил		+	+
VIII. Контроль (анализ) защищенности информации (АНЗ)				

АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе	+	+	+
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)				
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации		+	+
ОЦЛ.2	Контроль целостности информации, содержащейся в базах данных информационной системы			
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	+	+	+
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)		+	+
ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы			
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему			+
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему			
ОЦЛ.8	Контроль ошибочных действий пользователей по			

	вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях			
X. Обеспечение доступности информации (ОДТ)				
ОДТ.1	Использование отказоустойчивых технических средств			+
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы			+
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование		+	+
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации		+	+
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала		+	+
ОДТ.6	Кластеризация информационной системы и (или) ее сегментов			
ОДТ.7	Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации		+	+
XI. Защита среды виртуализации (ЗСВ)				
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры		+	+
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией			
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных		+	+

ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций		+	+
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры		+	+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	+	+	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей	+	+	+
XII. Защита технических средств (ЗТС)				
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам			
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	+	+	+
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)			+
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)				
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы		+	+

ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом			
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	+	+
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)			
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	+	+	+
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами			
ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода		+	+
ЗИС.8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи		+	+
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации		+	+
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам			
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты		+	+

	от подмены сетевых устройств и сервисов			
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю		+	+
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя		+	+
ЗИС.14	Использование устройств терминального доступа для обработки информации			
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации		+	+
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов			
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы		+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения			
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти			
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	+	+	+
ЗИС.21	Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы			+
ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы		+	+
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями		+	+
ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором		+	+

	временного интервала неактивности сетевого соединения			
ЗИС.25	Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды)			
ЗИС.26	Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем			
ЗИС.27	Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации			
ЗИС.28	Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы			
ЗИС.29	Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы			
ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе	+	+	+

"+" - мера защиты информации включена в базовый набор мер для соответствующего класса защищенности информационной системы.

Меры защиты информации, не обозначенные знаком "+", применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер защиты информации в информационной системе соответствующего класса защищенности.".

Лабораторная работа № 6
«Определение актуальных угроз безопасности ИС»

Цель работы – освоить методику определения актуальных угроз безопасности информации в ИС, предложенной ФСТЭК.

Введение

Использование класса защищенности ИС, позволяет определить лишь базовый набор мер защиты информации. Для использования уточненного адаптированного базового набора мер защиты информации, необходимо знать актуальные угрозы.

Рассмотрим методический документ ФСТЭК, который устанавливает единый методический подход к определению угроз безопасности информации в государственных информационных системах, защита информации в которых обеспечивается в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

Методика предназначена для:

- органов государственной власти, органов местного самоуправления и организаций, являющихся в соответствии с законодательством РФ обладателями информации, заказчиками и (или) операторами информационных систем;
- организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по созданию (проектированию) информационных систем;
- организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по защите информации в ходе создания (проектирования) и эксплуатации информационных систем;
- организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по аттестации (оценке соответствия) информационных систем требованиям о защите информации.

Источники угроз разделены на три типа:

- антропогенные источники (антропогенные угрозы);
- техногенные источники (техногенные угрозы);
- стихийные источники (угрозы стихийных бедствий, иных природных явлений).

В качестве источников антропогенных угроз безопасности информации могут выступать:

- лица, осуществляющие преднамеренные действия с целью доступа к информации (воздействия на информацию), содержащейся в информационной системе, или нарушения функционирования информационной системы или обслуживающей ее инфраструктуры (преднамеренные угрозы безопасности информации);

- лица, имеющие доступ к информационной системе, не преднамеренные действия которых могут привести к нарушению безопасности информации (непреднамеренные угрозы безопасности информации).

Для информационных систем, в которых целью защиты является обеспечение целостности и доступности обрабатываемой информации, в обязательном порядке подлежат оценке техногенные угрозы, связанные с отказами или сбоями в работе технических средств или программного обеспечения.

Для идентификации угроз безопасности информации в информационной системе определяются:

- возможности (тип, вид, потенциал) нарушителей, необходимые им для реализации угроз безопасности информации;
- уязвимости, которые могут использоваться при реализации угроз безопасности информации (включая специально внедренные программные закладки);
- способы (методы) реализации угроз безопасности информации;
- объекты информационной системы, на которые направлена угроза безопасности информации (объекты воздействия);
- результат и последствия от реализации угроз безопасности информации.

Разработка модели нарушителя

Целью оценки возможностей нарушителей по реализации угроз безопасности информации является формирование предположения о типах, видах нарушителей, которые могут реализовать угрозы безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования, а также потенциале этих нарушителей и возможных способах реализации угроз безопасности информации.

Типы нарушителей

Типы нарушителей определяются по результатам анализа прав доступа субъектов к информации и (или) к компонентам ИС, а также анализа возможностей нарушителей по доступу к компонентам ИС исходя из структурно-функциональных характеристик и особенностей функционирования ИС.

В зависимости от имеющихся прав доступа нарушители могут иметь легитимный физический (непосредственный) и (или) логический доступ к компонентам ИС и (или) содержащейся в них информации или не иметь такого доступа.

Анализ прав доступа проводится, как минимум, в отношении следующих компонент ИС:

- устройств ввода/вывода (отображения) информации;
- беспроводных устройств;

- программных, программно-технических и технических средств обработки информации;

- съемных машинных носителей информации;

- машинных носителей информации, выведенных из эксплуатации;

- активного (коммутационного) и пассивного оборудования каналов связи;

- каналов связи, выходящих за пределы контролируемой зоны.

С учетом наличия прав доступа и возможностей по доступу к информации и (или) к компонентам информационной системы нарушители подразделяются на два типа:

1) внешние нарушители (тип I) – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;

2) внутренние нарушители (тип II) – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам.

Наибольшими возможностями по реализации угроз безопасности обладают внутренние нарушители. Внешнего нарушителя необходимо рассматривать в качестве актуального во всех случаях, когда имеются подключения ИС к внешним информационно-телекоммуникационным сетям и (или) имеются линии связи, выходящие за пределы контролируемой зоны, используемые для иных подключений.

Виды и потенциал нарушителей

Угрозы безопасности информации в информационной системе могут быть реализованы следующими видами нарушителей:

1) специальные службы иностранных государств (блоков государств);

2) террористические, экстремистские группировки;

3) преступные группы (криминальные структуры);

4) внешние субъекты (физические лица);

5) конкурирующие организации;

6) разработчики, производители, поставщики программных, технических и программно-технических средств;

7) лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ;

8) лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.);

9) пользователи информационной системы;

10) администраторы информационной системы и администраторы безопасности;

11) бывшие работники (пользователи).

В качестве возможных целей (мотивации) реализации нарушителями угроз безопасности информации в информационной системе могут быть:

- нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики;

- реализация угроз безопасности информации по идеологическим или политическим мотивам;

- организация террористического акта;

- причинение имущественного ущерба путем мошенничества или иным преступным путем;

- дискредитация или дестабилизация деятельности органов государственной власти, организаций;

- получение конкурентных преимуществ;

- внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки;

- любопытство или желание самореализации;

- выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды;

- реализация угроз безопасности информации из мести;

- реализация угроз безопасности информации непреднамеренно из-за неосторожности или неквалифицированных действий.

Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом. Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования.

В зависимости от потенциала, требуемого для реализации угроз безопасности информации, нарушители подразделяются на:

- нарушителей, обладающих базовым (низким) потенциалом нападения при реализации угроз безопасности информации в информационной системе;

- нарушителей, обладающих базовым повышенным (средним) потенциалом нападения при реализации угроз безопасности информации в информационной системе;

- нарушителей, обладающих высоким потенциалом нападения при реализации угроз безопасности информации в информационной системе.

Возможные способы реализации угроз

Целью определения возможных способов реализации угроз безопасности информации является формирование предположений о возможных сценариях реализации угроз безопасности информации, описывающих последовательность (алгоритмы) действий отдельных видов нарушителей или групп нарушителей и применяемые ими методы и средства для реализации угроз безопасности информации.

Возможные способы реализации угроз безопасности информации зависят от структурно-функциональных характеристик и особенностей функционирования ИС.

Угрозы безопасности информации могут быть реализованы нарушителями за счет несанкционированного доступа на:

- объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах));
- объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы);
- объекты на прикладном уровне (системы управления базами данных, браузеры, web-приложения, иные прикладные программы общего и специального назначения);
- объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы);
- линии, (каналы) связи, технические средства, машинные носители информации.

Также возможны воздействия на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия).

Действия нарушителя в зависимости от его потенциала при реализации угроз безопасности информации предусматривают идентификацию и использование уязвимостей в микропрограммном, общесистемном и прикладном программном обеспечении, сетевом оборудовании, применяемых в ИС, а также в организации работ по защите информации и конфигурации ИС.

Определение актуальных угроз для информационной системы

Приведем неформализованное определение актуальной угрозы.

Угроза безопасности информации является актуальной, если для ИС с заданными структурно-функциональными характеристиками и особенностями функционирования существует вероятность реализации рассматриваемой угрозы нарушителем с соответствующим потенциалом и ее реализация приведет к неприемлемым негативным последствиям (ущербу) от нарушения конфиденциальности, целостности или доступности информации.

Идентифицированная угроза безопасности информации подлежит нейтрализации (блокированию), если она является актуальной для ИС, то есть в ИС с заданными структурно-функциональными характеристиками и особенностями функционирования существует вероятность (возможность) реализации рассматриваемой угрозы нарушителем с соответствующим потенциалом и ее реализация приведет к неприемлемым негативным последствиям (ущербу).

Если имеется необходимая информация, то говорят о вероятности реализации угрозы. Если используют экспертный подход, то говорят о возможности реализации угрозы.

Актуальные угрозы безопасности информации в обязательном порядке включаются в модель угроз безопасности информации.

Ниже приведена формализованная процедура, позволяющая относительно однозначно определить: угроза актуальна или нет.

Введем такие обозначения (номер угрозы опускаем).

Шкала для угрозы безопасности ШУА(АК, НАК), содержащая два уровня – АК (угроза актуальная), НАК (угроза неактуальная);

Зависимость угрозы безопасности (УБА) от двух факторов

$$\text{УБА}(Z, U), \qquad (6.1)$$

где Z – возможность реализации угрозы безопасности информации; U – степень возможного ущерба при реализации угрозы.

Фактор Z определяется 3-х уровневой шкалой вида (В, С, Н), где В – высокий уровень, С – средний уровень, Н – низкий уровень. Определение этих уровней приведено ниже.

Фактор U определяется 3-х уровневой шкалой ущерба вида (В, С, Н), где В – высокий, С – средний, Н – низкий уровни. Определение этих уровней берется из описания уровней этой шкалы:

высокий – в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции;

средний – в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций;

низкий – в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия. Информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

Обратим внимание на описания этих уровней, которые состоят из двух предложений. Первые предложения отличаются одним словом: высокий связан со словом «существенные», средний с «умеренные», а низкий со «значительные». Второе предложение поясняет значения этих слов через выполнение функций.

Например, если ИС не может выполнять хотя бы одну из возложенных на нее функцию, то это умеренные негативные последствия. Уровень ущерба будет средний.

При определении степени возможного ущерба необходимо исходить из того, что в зависимости от целей и задач, решаемых информационной системой, видов обрабатываемой информации, воздействие на конфиденциальность, целостность или доступность каждого вида информации, содержащейся в информационной системе, может привести к различным видам ущерба. При этом для разных обладателей информации и операторов будут характерны разные виды ущерба.

При экспертном подходе зависимость (6.1) определяется таблицей 6.1.

Таблица 6.1

Определение уровня актуальности угрозы безопасности

Z / *U*	Низкий	Средний	Высокий
Низкий	НАК	НАК	АК
Средний	НАК	АК	АК
Высокий	АК	АК	АК

Например, если возможность реализации угрозы безопасности информации (*Z*) имеет уровень – средний, а степень возможного ущерба при реализации угрозы (*U*) имеет уровень – высокий, то угроза будет иметь уровень АК – актуальная.

Фактор *Z* сам зависит от двух других факторов

$$Z(Y, G), \qquad (6.2)$$

где *Y* – уровень защищенности ИС; *G* – потенциал нарушителя. Уровень защищенности описывается 3-х уровневой шкалой вида: В, С, Н.

При функционировании ИС рассматривается два режима: проектный, когда определяется проектная защищенность ИС; эксплуатационный, когда определяется эксплуатационная защищенность ИС.

Для обоих этих режимов предлагаются 3-х уровневые шкалы. В качестве примера приведем шкалу для проектной защищенности:

а) информационная система имеет высокий уровень проектной защищенности, если не менее 80% характеристик информационной системы соответствуют уровню «высокий»;

б) информационная система имеет средний уровень проектной защищенности, если не выполняются условия по пункту а) и не менее 90% характеристик информационной системы соответствуют уровню не ниже «средний»;

в) информационная система имеет низкий уровень проектной защищенности, если не выполняются условия по пунктам а) и б).

Уровни шкалы для потенциала нарушителя имеют такой вид: базовый (низкий), базовый повышенный (средний), высокий. При экспертном подходе зависимость (6.2) определяется таблицей 6.2.

Результат реализации угрозы безопасности информации определяется воздействием угрозы на каждое свойство безопасности информации (конфиденциальность, целостность, доступность) в отдельности.

Таблица 6.2

Возможность реализации угрозы

G / *Y*	Высокий	Средний	Низкий
Базовый (низкий)	Низкая	Средняя	Высокая
Базовый повышенный (средний)	Средняя	Высокая	Высокая
Высокий	Высокая	Высокая	Высокая

При обработке в ИС двух и более видов информации (служебная тайна, персональные данные, налоговая тайна, иные установленные законодательством Российской Федерации виды информации) воздействие на конфиденциальность, целостность, доступность определяется отдельно для каждого вида информации, содержащейся в ИС.

Рассмотрим пример

Пусть уровень потенциала нарушителя (G) равен – высокий; уровень проектной защищенности (Y) – средний; уровень степени возможного ущерба (U) – средний.

Тогда, используя таблицу 6.2 определим, что уровень возможности реализации угрозы (Z) равен – высокий.

Используя таблицу 6.1, определим, что уровень угрозы безопасности информации – АК (актуальная).

Данную угрозу необходимо включить в модель угроз и блокировать средствами защиты.

Содержание лабораторной работы

1. Исходные данные лабораторной работы по своему варианту взять из таблицы 6.3.
2. Исходя из потенциала нарушителя и уровня проектной или эксплуатационной защищенности, по таблице 6.2 определить уровень возможности реализации угрозы.
3. Исходя из полученного уровня возможности реализации угрозы и заданного уровня степени возможного ущерба, по таблице 6.1 определить уровень актуальности угрозы безопасности.

Оформить лабораторную работу.

Список контрольных вопросов

1. Для чего необходимо знать актуальные угрозы безопасности ИС.
2. Назвать типы источников угроз и дать им характеристику.
3. Что нужно определить для идентификации угроз безопасности информации.
4. Что включает в себя модель нарушителя.
5. Типы нарушителей и к каким компонентам ИС они могут иметь доступ.
6. Виды нарушителя.
7. Что такое потенциал нарушителя и его уровни.
8. Возможные способы реализации угроз.
9. Дать определение актуальной угрозы.
10. Чем вероятность реализации угрозы отличается от возможности реализации угрозы.
11. В чем различие между эксплуатационным и проектным уровнем защищенности ИС.
12. Вопросы по определению актуальности угроз безопасности ИС.

Варианты лабораторной работы

Таблица 6.3

№	G	Y	U
1	H	B	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции
2	B	C	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции
3	C	B	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций
4	B	H	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступ-

			ности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций
5	Н	С	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия. Информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств
6	Н	В	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия. Информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств
7	В	С	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции
8	С	В	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций
9	В	Н	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций
10	Н	С	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия. Информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или вы-

			полнение функций возможно только с привлечением дополнительных сил и средств
11	В	Н	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции
12	С	В	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций
13	В	С	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций
14	Н	В	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции
15	С	Н	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции
16	В	С	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций
17	С	В	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций

18	В	Н	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия. Информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств
19	Н	С	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия. Информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств
20	Н	В	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции
21	В	С	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций
22	С	В	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций
23	В	Н	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия. Информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств
24	Н	С	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступ-

			ности) возможны существенные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции
25	В	Н	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций
26	С	В	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций
27	В	С	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции
28	Н	В	в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций

Практическое занятие № 1
«Правовое обеспечение информационной безопасности»

Данное практическое занятие рекомендуется провести после 4-й лабораторной работы.

Лекционное содержание занятия

Введение

Правовое обеспечение информационной безопасности и защиты информации на федеральном уровне включает в себя:

- федеральные законы,
- указы Президента РФ,
- постановления и распоряжения Правительства РФ,
- приказы различных министерств и ведомств.

Основными ФЗ, связанными с защитой информации и информационной безопасностью, являются:

- ФЗ № 149 от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации» в редакции от 03.04.2020 г.;
- ФЗ № 54-85-1 от 21.07.1993 г. «О государственной тайне» в редакции от 29.07.2018 г.;
- ФЗ № 98 от 29.07.2004 г. «О коммерческой тайне» в редакции от 18.04.2018 г.;
- ФЗ № 152 от 27.07.2006 г. «О персональных данных» в редакции от 01.07.2020 г.;
- ФЗ № 63 от 06.04.2011 г. «Об электронной подписи» в редакции, действующей с 31.12.2017 г.;
- ФЗ № 187 от 26.07.2017 г. «О безопасности критической информационной инфраструктуры РФ» и др.

Опишем кратко механизм введения федеральных законов на примере ФЗ «О персональных данных»:

1) принимается Государственной Думой РФ (8.07.2006);
2) одобряется Советом Федерации (14.07.2006);
3) утверждается Президентом РФ, после чего ему присваивается номер с датой (от 27.07.2006 № 152-ФЗ);
4) вводится с момента опубликования (дата утверждения Президентом РФ) или с другой датой. Например, рассматриваемый закон введен в действие с 27.01.2007 года.

Примеры правового обеспечения

Вопросы информационной безопасности учитывает и Уголовный кодекс РФ (УК РФ). В гл. 28 «Преступления в сфере компьютерной информации» УК РФ имеются три статьи:

1. Ст. 272 «Неправомерный доступ к компьютерной информации»: неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, – наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

2. Ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ»: создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

3. Ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»: нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок до четырех лет.

Учитывая важность вопросов, связанных с кибербезопасностью, в последнее время формируется нормативная база в этом направлении. В связи с этим кратко опишем Указ Президента РФ «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» от 15.01.2013 № 31.

В этом Указе информационные ресурсы – это информационные системы и информационно-телекоммуникационные сети, находящиеся на территории РФ и в дипломатических представительствах и консульских учреждениях РФ за рубежом. Основными задачами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ определены:

а) прогнозирование ситуации в области обеспечения информационной безопасности РФ;

б) обеспечение взаимодействия владельцев информационных ресурсов РФ, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;

в) осуществление контроля степени защищенности критической информационной инфраструктуры (КИИ) РФ от компьютерных атак;

г) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов РФ.

В развитие приведенного указа от 15.01.2013 № 31, в декабре 2014 года Президентом страны была утверждена концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (СОПКА).

В соответствии с этой концепцией основными функциями системы являются:

- выявление признаков проведения компьютерных атак,
- определение их источников и другой связанной информации,
- прогнозирование ситуации в области обеспечения информационной безопасности РФ,
- сбор и анализ информации о компьютерных атаках в отношении информационных ресурсов РФ,
- осуществление мероприятий по оперативному реагированию на атаки и ликвидации их последствий.

В ФЗ № 187 «О безопасности критической информационной инфраструктуры РФ» отмечается, что устанавливается обязательное требование о внедрении государственной системы обнаружения, предупреждения и ликвидации последствий кибератак на объекты КИИ. Это еще раз подтверждает значимость и актуальность вопросов кибербезопасности этих объектов для Российской Федерации.

В 2016 году была создана доктрина информационной безопасности РФ, утвержденная указом Президента от 05.12.2016 № 646. В этой доктрине отмечается, что «состояние информационной безопасности в области государственной и общественной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом кибератак на объекты КИИ».

Все это подтверждает значимость и актуальность вопросов кибербезопасности объектов КИИ для РФ и важность правового обеспечивания этих вопросов.

Частично компоненты правового обеспечения по защите информации уже рассмотрены ранее (ФЗ «Об информации, информационных технологиях и о защите информации», Указ Президента РФ от 06.03.1997 № 188 с изменениями от 23.09.2005 г. и др.).

Более подробно рекомендуется обсудить ФЗ № 152 от 27.07.2006 г. «О персональных данных» в редакции от 01.07.2020 г. Для этого необходимо заранее дать задание студентам подготовить этот вопрос.

Список контрольных вопросов

1. Назовите компоненты правового обеспечения защиты информации на федеральном уровне.
2. Перечислите основные федеральные законы, связанные с информационной безопасностью.
3. Опишите механизм введения федеральных законов.
4. Какие статьи, связанные с информационной безопасностью, присутствуют в уголовном кодексе РФ.
5. Приведите примеры Указов Президента РФ, связанных с информационной безопасностью.
6. Для чего выделяют категории персональных данных.
7. Особенности обработки персональных данных.
8. Что такое ИСПДн, виды ИСПДн.
9. Сколько уровней защищенности персональных данных и от каких факторов они зависят.

Практическое занятие № 2
«Организационное обеспечение информационной безопасности»

Данное практическое занятие рекомендуется провести после занятия № 1, посвященное правовому обеспечению информационной безопасности.

Лекционное содержание занятия

Введение

В организационном обеспечение по защите информации и информационной безопасности можно выделить три направления:

- совокупность органов государственной власти и управления, связанных с информационной безопасностью;
- структуры и их функции в организациях и на предприятиях различных форм собственности, ответственных за защиту информации;
- нормативно-правовые документы, обеспечивающие организационные меры по защите информации.

Организационные меры обеспечения информационной безопасности и защиты информации – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией, нарушения ее целостности и проявление различных угроз.

Организационные меры обеспечивают:

1) организацию охраны, режима, работу с кадрами и документами;

2) использование технических средств безопасности;

3) информационно-аналитическую деятельность по выявлению различных угроз и выработки мер по обеспечению защиты информации.

При организации работы с сотрудниками, помимо подбора и расстановки кадров, необходимо их обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности и т. д.

Организация работы с документами и документированной информацией включает организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение. Опираясь на государственные правовые акты и учитывая интересы своего предприятия, разрабатываются собственные нормативно-правовые документы, ориентированные на обеспечение информационной безопасности.

К основным таким документам относятся:

1) перечень сведений, составляющих конфиденциальную информацию;

2) положение о сохранении конфиденциальной информации;

3) инструкция о порядке допуска сотрудников к сведениям, составляющих конфиденциальную информацию;

4) положение о специальном делопроизводстве и документообороте;

5) обязательство сотрудника о сохранении конфиденциальной информации.

Специфической областью организационных мер является организация защиты информационных систем и сетей, которая определяет порядок и схему функционирования основных подсистем, использование устройств и ресурсов, взаимоотношения пользователей, разработчиков и обслуживающего персонала между собой в соответствии с нормативно-правовыми требованиями и правилами. Эти вопросы будут рассмотрены ниже.

Функции органов государственной власти, обеспечивающих информационную безопасность в Российской Федерации

Основным государственным органом, определяющим политику РФ в сфере безопасности страны в целом и информационной безопасности в частности, является Совет безопасности РФ.

Функции и состав Совета определяются ФЗ № 390 от 18.12.2010 года с изменениями на 06.02.2020 год.

Совет безопасности РФ, возглавляемый Президентом РФ, рассматривает вопросы внутренней и внешней политики РФ в области обеспечения безопасности, стратегические проблемы государственной, экономической, общественной, оборонной, информационной, экологической и иных видов безопасности.

Основными функциями Совета безопасности РФ являются:

1) формирование государственной политики в области обеспечения безопасности и контроль за ее реализацией;

2) прогнозирование, выявление, анализ и оценка угроз безопасности, оценка военной опасности и военной угрозы, выработка мер по их нейтрализации;

3) подготовка предложений Президенту Российской Федерации и др.

Для решения задач, связанных с обеспечением информационной безопасности, в составе Совета безопасности РФ функционирует созданное Управление информационной безопасности (одно из профильных управлений), а также Межведомственная комиссия по информационной безопасности.

Функциями Управления информационной безопасности являются:

1) подготовка предложений Совету безопасности РФ по выработке и реализации основных направлений политики государства в области обеспечения информационной безопасности РФ;

2) анализ и прогнозирование ситуации в области информационной безопасности РФ;

3) выявление источников опасности, оценка внешних и внутренних угроз информационной безопасности и подготовка предложений Совету безопасности РФ по их предотвращению;

4) рассмотрение в установленном порядке проектов федеральных целевых программ, направленных на обеспечение информационной безопасности РФ, подготовка соответствующих предложений;

5) участие в подготовке материалов по вопросам обеспечения информационной безопасности РФ для ежегодного послания Президента РФ Федеральному Собранию и для докладов Президента РФ;

6) подготовка предложений по проектам решений Совета Безопасности и информационно-аналитических материалов к его заседаниям по вопросам обеспечения информационной безопасности РФ;

7) подготовка предложений Совету безопасности РФ по разработке проектов нормативных правовых актов, направленных на обеспечение информационной безопасности РФ.

Функции ФСТЭК

Ведущим государственным учреждением, непосредственно ответственным за реализацию государственной политики в сфере информационной безопасности и защиту государственных интересов на общенациональном уровне, является Федеральная служба по техническому и экспортному контролю (ФСТЭК). Данная организация, известная до 2004 года как Государственная техническая комиссия при Президенте РФ (Гостехкомиссия РФ), была создана в январе 1992 года на базе Гостехкомиссии СССР по противодействию иностранным техническим разведкам, которая, в свою очередь ведет отсчет своего существования с декабря 1973 года.

Произошедшее в 1992 году преобразование было связано со сменой политических приоритетов, интенсивным развитием электронных коммуникаций и средств вычислительной техники, отменой государственной монополии на многие сферы экономической и технической деятельности, развитием рыночных отношений, расширением международных связей и другими факторами. ФСТЭК, ранее подчинявшаяся напрямую Президенту РФ, в процессе административной реформы вошла в состав министерства обороны РФ, но ее деятельностью управляет Президент. ФСТЭК является коллегиальным органом – в состав Коллегии входят 19 представителей различных министерств и ведомств (главным образом, в ранге заместителей министров и директоров департаментов).

Основными функциями ФСТЭК являются:

1) проведение единой технической политики и координация работ по защите информации;

2) организация и контроль за проведением работ по защите информации в органах государственного управления, объединениях, концернах, на предприятиях, в организациях и учреждениях (независимо от форм собственности) от:

- утечки по техническим каналам,
- несанкционированного доступа к информации, обрабатываемой техническими средствами,

- специальных воздействий на информацию с целью ее уничтожения и искажения;

3) поддержание системы лицензирования деятельности предприятий, организаций и учреждений по осуществлению мероприятий и (или) оказанию услуг в области защиты информации и сертификации средств защиты информации.

Для реализации функций по лицензированию в составе ФСТЭК функционируют региональные управления (по федеральным округам), а также отраслевые аттестационные центры.

Отметим одну из важных функций ФСТЭК, а именно формирование банка данных угроз (информационное письмо № 240/22/879 от 06.03.2015). Банк данных включает базу данных уязвимостей программного обеспечения, а также перечень и описание угроз безопасности информации.

Другие органы управления

Важную роль в системе органов государственной власти, отвечающих за решение задач информационной безопасности, играет Служба специальной связи и информации (Спецсвязь России), созданная в 2004 г. в рамках Федеральной службы охраны (ФСО) на базе упраздненного Федерального агентства правительственной связи и информации (ФАПСИ). Эта Служба призвана обеспечивать функционирование президентской связи, организацию, эксплуатацию и развитие специальной связи для государственных органов и решать другие аналогичные задачи.

Основными задачами Службы спецсвязи являются:

1) проведение работ по защите технических средств специальной связи, устанавливаемых в категорированных помещениях государственных органов, включая особо важные;

2) организация в системе специальной связи шифровальной деятельности, отнесенной к компетенции спецсвязи России;

3) участие в разработке нормативной технической документации по вопросам защиты информации в системах специальной связи;

4) участие в разработке и реализации мер по обеспечению информационной безопасности Российской Федерации, защите сведений, составляющих государственную тайну;

5) участие в создании, обеспечении и развитии системы электронного документооборота государственных органов с использованием удостоверяющих центров;

6) организация и проведение мероприятий по предотвращению утечки по техническим каналам информации в системах специальной связи, информационно-технологических, информационно-аналитических и информационно-телекоммуникационных системах, находящихся в ведении спецсвязи России;

7) выполнение требований обеспечения информационной безопасности объектов государственной охраны.

За вопросы криптографической защиты информации и других вопросов по информационной безопасности отвечает Федеральная служба безопасности (ФСБ) в лице Центра защиты информации и специальной связи, Управления компьютерной и информационной безопасности, Института криптографии, связи и информатики при Академии ФСБ и других подразделений.

Вопросы повышения качества информационной работы и информационной безопасности решают также другие федеральные органы (в пределах своей компетенции).

Министерство цифрового развития, связи и массовых коммуникаций РФ осуществляет и организует следующие виды работ в сфере информационной безопасности:

1) подтверждение подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей;

2) ведение единого государственного реестра сертификатов ключей подписей удостоверяющих центров и реестра сертификатов ключей подписей уполномоченных лиц федеральных органов государственной власти, а также обеспечение доступа к ним граждан, организаций, органов государственной власти и органов местного самоуправления;

3) выполнение функции государственного заказчика научно-технических и инвестиционных программ и проектов в сфере информационных технологий.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных. В полномочия данного органа входит пресечение нарушений, которые могут возникать при обработке персональных данных граждан РФ и многих других вопросов.

Важную роль играет Центральный банк РФ в составе которого функционирует Главное управление безопасности и защиты информации.

В системе законодательной власти основным структурным подразделением, призванным решать вопросы формирования и реализации государственной политики в сфере информационной безопасности, является Комитет по безопасности Государственной думы Федерального собрания Российской Федерации. В составе этого Комитета функционирует Подкомитет по информационной безопасности. В законодательной работе в рамках этого Комитета принимают участие:

а) специалисты и руководители профильных подразделений ФСБ, ФСО, ФСТЭК, МВД и других ведомств;

б) руководители Совета безопасности РФ и других правительственных органов;

в) представители общественных организаций, фондов и профессиональных объединений;

г) представители крупных коммерческих компаний – лидеров в развитии организации и технологий информационной безопасности (в том числе банков, технологических компаний и др.);

д) представители ведущих научно-исследовательских учреждений и учебных заведений.

Утверждение и ввод в действие национальных стандартов РФ осуществляет Федеральное агентство по техническому регулированию и метрологии (Стандартинформ).

Более подробно рекомендуется обсудить функции и результаты деятельности ФСТЭК. Для этого необходимо заранее дать задание студентам подготовить этот вопрос.

Список контрольных вопросов

1. Основные направления в организационном обеспечение по защите информации и информационной безопасности.
2. Приведите органы государственной власти, обеспечивающих информационную безопасность в Российской Федерации.
3. Основные функции Совета безопасности РФ.
4. Основные функции ФСТЭК.
5. Приведите примеры приказов ФСТЭК.
6. Основные задачи Службы спецсвязи РФ.
7. Какое агентство отвечает за ввод в действие национальных стандартов РФ.

Список рекомендуемой литературы

Основная литература

1. Краковский Ю.М. Информационная безопасность и защита информации. Иркутск: Изд-во ИрГУПС, 2016. 224 с.
2. Краковский, Ю. М. Защита информации : учебное пособие / Ю. М. Краковский. — Ростов н/Д : Феникс, 2017. — 347 с.
3. Ерохин, В. В. Безопасность информационных систем : учебное пособие / В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко. — 2-е изд. — Москва : ФЛИНТА, 2015. — 182 с.

Дополнительная литература

4. Мельников, Д. А. Информационная безопасность открытых систем : учебник / Д. А. Мельников. — 2-е изд. — Москва : ФЛИНТА, 2014. — 448 с.
5. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам : справочное пособие / Г. А. Бузов. — Москва : Горячая линия-Телеком, 2018. — 586 с.
6. Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 256 с.
7. Долозов, Н. Л. Программные средства защиты информации : учебное пособие / Н. Л. Долозов, Т. А. Гультяева. — Новосибирск : НГТУ, 2016. — 63 с.
8. Программно-аппаратные средства защиты информации : учебное пособие / Л. Х. Мифтахова, А. Р. Касимова, В. Н. Красильников [и др.]. — Санкт-Петербург : Интермедия, 2018. — 408 с.

Краковский Юрий Мечеславович

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Методическое пособие