Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный университет геосистем и технологий»
(СГУГиТ)

А. В. Троеглазова

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Утверждено редакционно-издательским советом университета
в качестве практикума для обучающихся по направлению подготовки
10.03.01 Информационная безопасность (уровень бакалавриата)

Новосибирск
СГУГиТ
2022

УДК 004.056.5(075.8)
Т703

Рецензенты: кандидат юридических наук, доцент СибГУТИ *Е. А. Овчинникова*

кандидат технических наук, доцент СГУГиТ *Д. Н. Титов*

Троеглазова, А. В.

Т703 Основы информационной безопасности : практикум / А. В. Троеглазова. – Новосибирск : СГУГиТ, 2022. – 40 с. – Текст : непосредственный.

ISBN 978-5-907513-70-9

Практикум подготовлен доктором философии (PhD), доцентом А. В. Троеглазовой на кафедре информационной безопасности СГУГиТ.

Рассматриваются вопросы организации практических работ по дисциплине «Основы информационной безопасности». Содержатся рекомендации по выполнению практических работ и контрольные вопросы для защиты практических работ обучающихся по основам информационной безопасности.

Практикум по дисциплине «Основы информационной безопасности» предназначен для обучающихся по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата).

Рекомендован к изданию кафедрой информационной безопасности, Ученым советом Института оптики и технологий информационной безопасности СГУГиТ.

Печатается по решению редакционно-издательского совета СГУГиТ

УДК 004.056.5(075.8)

ISBN 978-5-907513-70-9

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Основной *целью практикума* является формирование базовых компетенций и развитие у обучающихся способности анализировать, мыслить и использовать фундаментальные знания в процессе выполнения практических работ по основам информационной безопасности.

Задачи практикума – ознакомление обучающихся с основными разделами информационной безопасности, подходами к изучению понятийного аппарата, национальными интересами в сфере информационной безопасности, угрозами национальной безопасности страны и выбранных организаций.

Настоящий практикум является руководством к выполнению шести практических работ по дисциплине «Основы информационной безопасности» для обучающихся по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата).

Описание практических работ включает в себя цель работы, необходимое оборудование, длительность выполнения, порядок выполнения. В начале каждой работы дан краткий теоретический материал, помогающий обучающемуся в осознанном выполнении заданий.

Обучающийся может приступить к выполнению практической работы только после изучения лекционного материала и материала, приведенного в теоретической части практической работы. Для самостоятельной оценки уровня подготовленности в каждой практической работе приведены контрольные вопросы.

Также работа содержит приложение, в котором приведены справочные данные, необходимые обучающимся при выполнении практических заданий. Если материал по некоторым вопросам несколько выходит за пределы программы учебной дисциплины, то обучающийся может воспользоваться библиографическими источниками из приведенного списка [1–8].

ТРЕБОВАНИЯ К ОТЧЕТУ ПО ПРАКТИЧЕСКОЙ РАБОТЕ

Отчет по практической работе должен включать в себя следующие элементы:

1) номер практической работы;

2) название практической работы;

3) цель выполнения практической работы;

4) порядок выполнения работы;

5) результаты, полученные в ходе выполнения практической работы, в том числе результаты литературного анализа;

6) выводы в целом по практической работе согласно поставленной цели.

Практическая работа № 1.
ИЗУЧЕНИЕ ПОНЯТИЙНОГО АППАРАТА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель работы: проанализировать стандарт ГОСТ Р 53114–2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения [1] и составить интеллект-карту для выбранных терминов и их определений.

Оборудование: учебный персональный компьютер.

Количество часов: 2 часа.

Общие теоретические сведения

Термины и их определения для изучения основ информационной безопасности приведены в [1].

Под информационной безопасностью понимается состояние защищенности информации как объекта рассмотрения, при котором обеспечиваются три основных условия – конфиденциальность, целостность и доступность.

Соблюдение конфиденциальности предполагает обеспечение доступа к информации только тех субъектов информационных отношений, которые имеют на это право. Состояние, когда обеспечивается сохранение неизменности содержания информации, называют *целостностью информации*. Обеспечение возможности беспрепятственного доступа к информации всех субъектов, которые имеют право такого доступа, называют *доступностью информации*.

При этом для любого вида информации возможна ситуация, характеризующаяся наличием условий и факторов, создающих реальную или потенциальную опасность обеспечения конфиденциальности, доступности и целостности информации. Такую совокупность условий и факторов называют *угрозой информационной безопасности*. А потенциальных злоумышленников, создающих эту опасность, называют *источниками угроз*.

Обеспечение безопасности информации в любой организации независимо от вида ее деятельности должно носить комплексный характер.

При этом можно выделить четыре уровня защиты информации [2–6]:

1 уровень – законодательный;

2 уровень – административный;

3 уровень – процедурный;

4 уровень – программно-технический.

На законодательном уровне рассматриваются законы, подзаконные акты, нормативные документы, документация международного сообщества в сфере информационного права, которые регламентируют порядок защиты информации, контроль эффективности действующей системы защиты информации, виды ответственности за нарушение законодательства в сфере информационного права.

В рамках административного уровня разрабатывается и применяется комплекс мер по обеспечению защиты информации непосредственно в организации высшим руководством. Разработка, утверждение, внедрение и оценка эффективности применения инструкций по работе персонала с целью обеспечения защиты информации в организации осуществляется в рамках процедурного уровня защиты информации. Деятельность по разработке, аттестации, применению готовых программно-аппаратных и технических средств защиты информации осуществляется в рамках программно-технического уровня защиты информации в организации.

Для изучения понятийного аппарата в разных сферах деятельности, в том числе в области информационной безопасности, применяются различные методы, но среди таких методов наиболее широкое распространение получил метод интеллект-карт.

Интеллект-карты (ментальные карты, карты мыслей) разработаны британским психологом Тони Бьюзеном. Их применение позволяет обеспечить осмысленность изучения теоретического материала и повысить степень его восприятия обучающимся. Для построения интеллект-карт необходимо придерживаться следующих правил.

1. Четко формулировать тему (термин) для построения интеллект-карты.

2. Графическое изображение темы (термина) должно представлять собой центральный образ, рисунок.

3. Подобрать все возможные ассоциации с выбранной темой (термином).

4. Произвести группировку ассоциаций по определенным признакам.

5. Произвести структурирование ассоциаций – подбор ключевых слов и/или ключевых фраз.

6. Произвести графическое структурирование – добавление ключевых ветвей к центральному образу.

7. Заполнить графическую структуру – добавить ответвления.

8. Произвести оживление графической структуры – добавить символику, ассоциирующуюся со словами.

9. Выделить структуру – выделить ключевые ветви цветными блоками.

10. Установить объективные связи между блоками и/или их элементами.

Пример интеллект-карты, составленный для термина «Информационная безопасность в интернете», представлен на рис. 1.1.

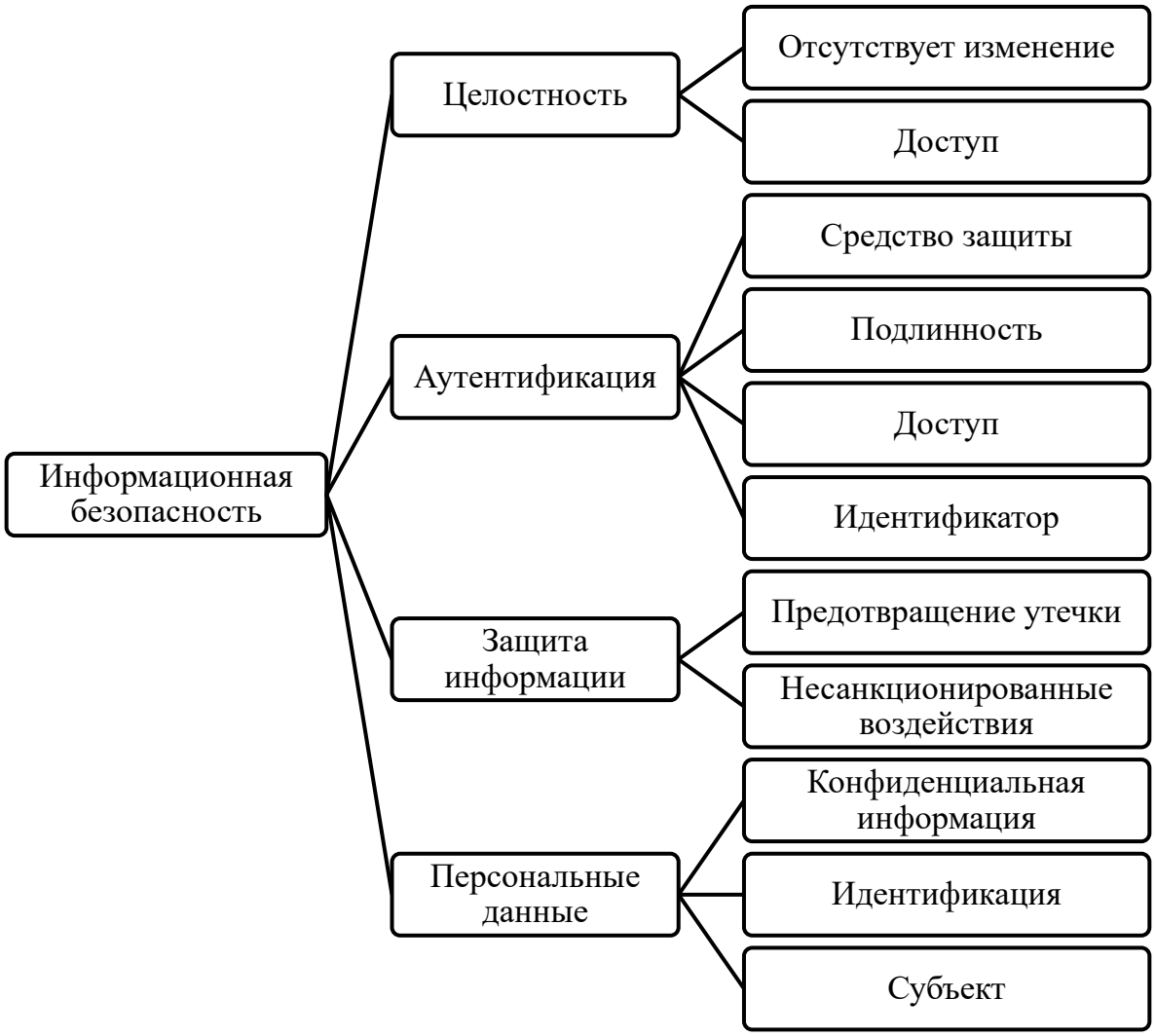

Рис. 1.1. Интеллект-карта термина
«Информационная безопасность в интернете»

Порядок выполнения работы

1. Изучить стандарт ГОСТ Р 53114–2008. Защита информации. Обеспечение информационной безопасности в организации [1].

2. Изучить основные термины и определения, составить в тетради по дисциплине глоссарий по десяти терминам и их определениям.

3. Разработать интеллект-карту для пяти выбранных вами терминов, применяемых в сфере информационной безопасности.

Отчет должен содержать следующую информацию:

1) номер и наименование работы;
2) цель работы;
3) задание;
4) глоссарий;
5) интеллект-карту;
6) вывод о проделанной работе.

Контрольные вопросы

1. Что называют информацией?
2. Какие виды информации вы знаете? Приведите их характеристику.
3. Дайте определение понятию «Информационная безопасность»?

Практическая работа № 2.
ИСТОРИЧЕСКИЕ ЭТАПЫ РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель работы: составить инфографику по этапам исторического развития информационной безопасности на основе литературных данных.

Оборудование: учебный персональный компьютер.

Количество часов: 2 часа.

Общие теоретические сведения

В целом можно выделить 7 этапов исторического развития информационной безопасности [2–6].

I этап – до 1816 г.

В связи с изобретением письменности этот этап характеризуется фиксацией сообщений на простейших материальных носителях и применением первых методов защиты такой информации с помощью криптографии и сокрытия. Так, например, в документах Индии, Египта и Месопотамии приведены данные, свидетельствующие о применении шифра перестановки и шифра простой замены при составлении писем и сообщений. К наиболее раннему зашифрованному сообщению относится рецепт глазури в гончарном производстве, нанесенный в зашифрованном виде на глиняную табличку в Месопотамии в XX в. до н. э.

II этап – 1816–1934 гг.

В этот период начинается бурное развитие как технических способов сохранения и передачи информации с помощью электрических сигналов и электромагнитных полей (появляется радио, телеграф, телефон), так и способов защиты при использовании технических каналов утечки информации (побочные изучения, наводки и т. д.). Поэтому для сохранения конфиденциальности передаваемой информации применяется помехоустойчивое шифрование с последующим декодированием сообщения. Это период раз-

вития промышленного и государственного шпионажа с применением различных технических средств разведки.

III этап – 1935–1945 гг.

Этот период характеризуется массовой информатизацией общества, внедрением автоматизированных систем обработки информации, созданием и расширением областей применения радиолокационных и гидроакустических средств. Защита информации в этот период осуществляется применением организационных и технических мер.

IV этап – 1946–1964 гг.

Первая электронно-вычислительная машина (ЭВМ) появилась в 1945 г. Разработана она была в США Дж. Моучли и Дж. Эккертом с применением электронным ламп. ЭВМ представляла собой комплекс программных, аппаратных и технических средств для автоматической обработки информации, расчетов и управления. Появление и повсеместное использование ЭВМ привело к увеличению доли финансовых преступлений в компьютерной сфере в 60-х гг. XX в., о чем свидетельствует множество публикаций в открытых источниках. Защита информации преимущественно осуществлялась путем физического ограничения доступа к оборудованию по сбору, обработке и передаче информации.

V этап – 1965–1972 гг.

В этот период разработаны и активно внедряются локальные информационно-коммуникационные сети, что позволило обеспечить доступ с одной машины ко всем компьютерам и периферийным устройствам, входящим в локальную сеть. Защита информации осуществляется путем администрирования и управления доступом к локальной сети, а также путем физического ограничения доступа к средствам сбора, обработки и передачи информации. Осуществляемая деятельность по защите информации направлена на предупреждение несанкционированного доступа к защищаемой организацией информации и установлением режима секретности.

VI этап – 1973–1984 гг.

Этап характеризуется повсеместным применением коммуникационных устройств, мобильных информационных технологий, что стало катализатором для появления сообществ хакеров, нацеленных на нанесение ущерба организациям и государствам с использованием информационных

технологий. В этот период наблюдается интенсификация процесса поиска, разработки и реализации способов и средств защиты информации по обеспечению ее целостности. Расширяет ассортимент применяемых средств защиты информации – технических, программных и организационных, широкое распространение получили криптографические методы защиты информации. Формируется новая отрасль международного и национального права в сфере защиты информации – информационное право.

VII этап – 1985 – настоящее время.

В данный период осуществляется переход процесса обеспечения безопасности информации с прикладного характера на научную основу благодаря комплексной обработке результатов накопленного опыта и знаний с применением научно-методологических методов. Информационная безопасность стала рассматриваться как комплексная система защиты информации, включающая в себя несколько подсистем:

– обеспечение режима секретности – работу со сведениями, составляющими государственную тайну;

– криптографическую защиту информации, передаваемую по каналам связи;

– противодействие техническим средствам разведки, заключающееся в обеспечении конфиденциальности информации от утечки ее по техническим каналам связи;

– защиту конфиденциальной информации, хранимую и обрабатываемую с использованием электронно-вычислительной техники и передаваемой по компьютерным сетям.

Порядок выполнения работы

1. Изучить литературные данные (книги, монографии, научные статьи, учебные пособия и т. д.) по вопросу исторического развития информационной безопасности.

2. Составить инфографику по заявленной теме, сформулировав основные этапы исторического развития, периоды, особенности, исторических личностей.

3. Подготовиться к защите практической работы с использованием инфографики.

Отчет должен содержать:

1) номер и наименование работы;

2) цель работы;

3) задание;

4) инфографика;

5) вывод о проделанной работе.

Контрольные вопросы

1. Приведите характеристику основных этапов развития информационной безопасности?

2. Как бы вы охарактеризовали особенности современного этапа развития информационной безопасности в Российской Федерации?

3. Какие криптографические способы защиты информации применяли на разных этапах развития информационной безопасности?

Практическая работа № 3.
АНАЛИЗ ДОКТРИНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель работы: провести анализ национальных интересов в информационной сфере и угроз их безопасности.

Оборудование: учебный персональный компьютер.

Количество часов: 2 часа.

Общие теоретические сведения

Главным документом страны, регламентирующим вопросы государственной политики в информационной сфере, является Доктрина информационной безопасности, введенная в действие Указом Президента РФ от 05.12.2016 № 646 [7]. Она заменила документ, действующий с начала 2000 г.

Доктрина информационной безопасности является правовым документом, отражающим национальные интересы страны, официальные взгляды государства на регулирование вопросов по обеспечению информационной безопасности, цели и задачи, принципы и направления развития. Доктрина состоит из пяти разделов. В ней рассматриваются следующие вопросы:

– основные положения, описывающие назначение доктрины и ее применение, основные термины и их определения;

– национальные интересы Российской Федерации;

– угрозы и состояние информационной безопасности;

– стратегические цели и направления обеспечения информационной безопасности страны;

– организационные основы обеспечения информационной безопасности.

К внешним угрозам относятся: наращивание возможностей информационно-технического виляния на инфраструктуру ряда иностранных государств в военной области, усиление деятельности иностранных организаций, осуществляющих техническую разведку.

К внутренним угрозам относятся: неудовлетворительное состояние отечественных отраслей промышленности и экономики, недостаточный уровень информатизации органов государственной власти, финансовых орга-

низаций, в сфере различных отраслей промышленности, здравоохранения, образования, сельского хозяйства и т. д. [7].

Порядок выполнения работы

1. Найти текст документа «Доктрина информационной безопасности» на сайте «КонсультантПлюс».

2. Изучить текст Доктрины [7] и заполнить табл. 3.1–3.3.

Таблица 3.1

Классификация национальных интересов в информационной сфере в зависимости от принадлежности интересов

Интересы личности	Интересы общества	Интересы государства

Таблица 3.2

Классификация национальных интересов в информационной сфере по важности интересов

Соблюдение конституционных прав и свобод, …	Информационное обеспечение государственной политики	Найти самостоятельно	Найти самостоятельно

Таблица 3.3

Классификация угроз информационной безопасности по общей направленности

Источники угроз	Конституционные права и свободы, общественное сознание личности		Информационное обеспечение государственной политики		Развитие государства		Безопасность информационных и телекоммуникационных средств и систем	
	Угрозы	Меры защиты	Угрозы	Меры защиты	Угрозы	Меры защиты	Угрозы	Меры защиты
Внутренние								
Внешние								

3. Оформить отчет о проделанной вами работе.

Отчет должен содержать следующую информацию:

1) номер и наименование работы;

2) цель работы;

3) заполненные три таблицы;

4) вывод о проделанной работе.

Контрольные вопросы

1. Приведите характеристику Доктрины информационной безопасности.

2. Чем Доктрина информационной безопасности, утвержденная в 2016 г., отличается от предыдущей версии?

3. Сформулируйте угрозы национальным интересам страны по состоянию на начало 2022 г.

Практическая работа № 4.
КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель работы: проанализировать угрозы информационной безопасности с учетом потенциальных нарушителей для выбранной организации.

Оборудование: учебный персональный компьютер.

Количество часов: 4 часа.

Общие теоретические сведения

Угрозы информационной безопасности классифицируют по различным признакам [2–6].

1. В зависимости от факторов возникновения угрозы могут быть основаны на естественных и на человеческих факторах (рис. 4.1).

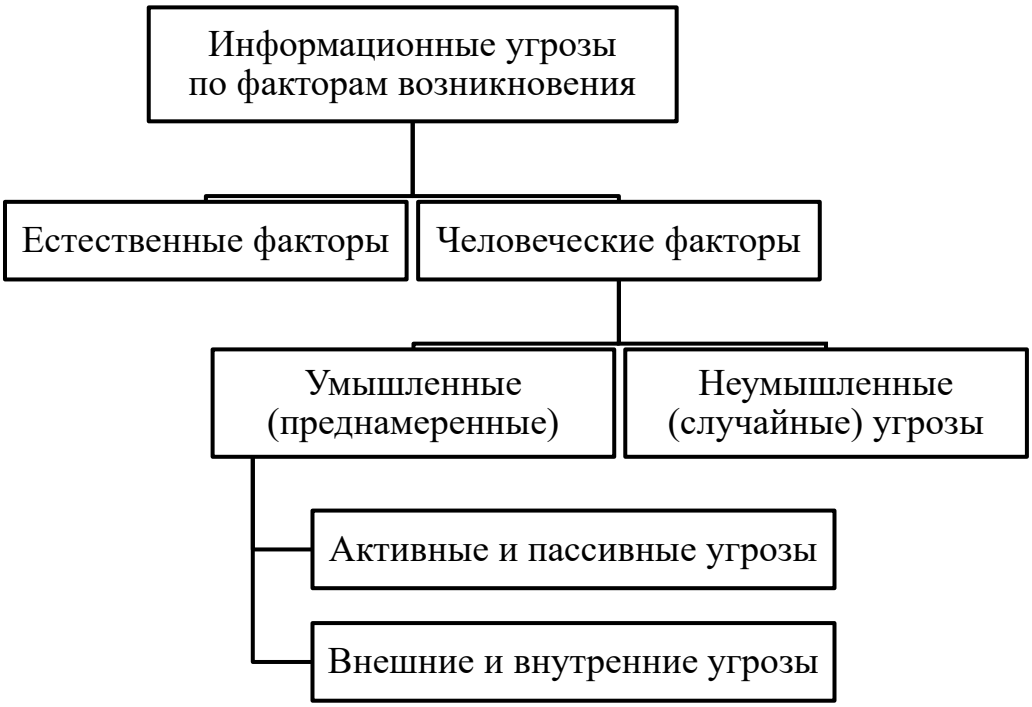

Рис. 4.1. Классификация угроз информационной безопасности по факторам возникновения

Угрозы, основанные на естественных факторах, не зависят от человека и имеют стихийный характер. К ним можно отнести угрозу наводнения, пожара и любого другого стихийного бедствия. Угрозы на основе человеческого фактора подразделяют на две основные группы: умышленные и неумышленные угрозы (рис. 4.2) [2–6].

Рис. 4.2. Классификация угроз сохранности информации

Неумышленные угрозы возникают в результате случайных (непреднамеренных) ошибок человека. Умышленные (преднамеренные) угрозы могут быть активными и пассивными. В качестве примера пассивной угрозы можно рассмотреть подслушивание, подсматривание, наблюдение и т. д. Реализация пассивной угрозы не нарушает деятельность объекта информа-

тизации в отличие от активных угроз, которые напрямую влияют на деятельность объекта информатизации и нарушают его работу.

2. По цели реализации угроз их классифицируют на три основные угрозы: нарушение конфиденциальности, целостности, доступности.

3. В зависимости от принципа воздействия на объект выделяют угрозы с использованием доступа субъекта системы к объекту и угрозы с использованием скрытых каналов.

4. По причине появления используемой ошибки защиты: неадекватность политики безопасности реальной системе, ошибки административного управления, ошибки в алгоритмах программ, ошибки реализации алгоритмов программ.

5. По используемым средствам атаки – непосредственное воздействие на объект атаки и воздействие на систему разрешений.

6. По объекту атаки: автоматизированные информационные системы (АИС) в целом, объекты системы, субъекты системы, каналы передачи данных.

Реализация угроз на объекты информатизации осуществляется различными способами: информационные, программно-математические, физические, радиоэлектронные, организационно-правовые. Информационные способы включают в себя противозаконный сбор и использование информации, несанкционированный доступ к информационным ресурсам, сокрытие информации, нарушение технологии обработки информации.

К программно-математическим способам относятся внедрение компьютерных вирусов, установка закладных устройств, уничтожение и модификация данных автоматизированных информационных системах.

Под физическими способами реализации угроз подразумевают уничтожение, разрушение и хищение носителей информации; перехват, дешифровка и навязывание ложной информации и т. д. К радиоэлектронным способам относятся: перехват информации в технических каналах ее утечки, внедрение устройств перехвата информации. Под организационно-правовыми способами реализации угроз безопасности подразумевают невыполнение требований, изложенных в законодательных и подзаконных актах, локальных документах организации, неправомерное ограничение доступа к документам.

Порядок выполнения работы

1. Из приведенного перечня (табл. 4.1) выбрать организацию для проведения анализа и по виду деятельности определить виды информации, которые необходимо защитить.

Таблица 4.1

Варианты объектов защиты

Вариант	Наименование организации
1	Завода железобетонных изделий
2	Торговый центр
3	Поликлиника
4	Университет
5	Научно-исследовательский институт
6	Предприятие по производству фармацевтических препаратов
7	Районный отдел полиции
8	Банк
9	Патентное бюро
10	Редакция научного издания
11	Научно-производственное предприятие
12	Склад текстильной продукции
13	Рекламное агентство
14	Производственный цех бурового оборудования
15	Птицефабрика
16	Республиканская библиотека
17	Музей изобразительных искусств
18	Средняя школа
19	Больница
20	Районный суд

2. Изучив лекционный материал по теме и теоретическую часть практической работы, для каждого вида защищаемой информации определить не менее 10 угроз информационной безопасности по обеспечению целост-

ности, конфиденциальности и доступности. Анализ представить в табличном варианте (табл. 4.2).

Таблица 4.2

Результаты анализа угроз безопасности информации в организации

_____

(наименование организации)

Вид защищаемой информации	Наименование угрозы	Тип информационной угрозы	Способ воздействия на информационный объект	Источник угрозы	Мера защиты информации от угрозы

Отчет должен содержать:

1) номер и наименование работы;
2) цель работы;
3) наименование организации, выбранной обучающимся;
4) заполненная табл. 4.2;
5) вывод о проделанной работе.

Контрольные вопросы

1. Что называют угрозой информационной безопасности?

2. Приведите классификацию угроз безопасности информации по различным признакам.

3. Каковы причины нарушения целостности, доступности и конфиденциальности информации?

4. Назовите и приведите характеристику источников появления угроз информационной безопасности.

5. Какие способы реализации угроз безопасности информации вы знаете? Приведите их характеристику.

Практическая работа № 5.
КЛАССИФИКАЦИЯ НАРУШИТЕЛЕЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Цель работы: изучить характеристику основных групп нарушителей, определить потенциальных нарушителей защиты рассматриваемого объекта информатизации.

Оборудование: учебный персональный компьютер.

Количество часов: 2 часа.

Общие теоретические сведения

Нарушителем считается физическое лицо, которое случайно или преднамеренно нарушило безопасность защищаемой информации при ее обработке в информационной системе. Действия нарушителя могут привести нарушению целостности, конфиденциальности, доступности защищаемых информационных ресурсов, созданию условий для последующей реализации несанкционированного доступа к защищаемой информации.

Действия нарушителя могут быть осуществлены в различных направлениях [2–6]:

– путем хищения, ознакомления и перехвата информации с целью нарушения ее конфиденциальности;

– изменение данных (их модификация) с целью нарушения целостности защищаемой информации;

– полное и частичное нарушение доступности информации путем применения различных технических, программных и аппаратных средств;

– изменений конфигураций и настроек средств защиты информации, применяемых в организации.

Нарушителей безопасности информации можно классифицировать на два типа: внешние и внутренние. Внешние нарушители, в отличие от внутренних, осуществляют свои атаки за пределами контролируемой зоны информационной системы. К внешним нарушителям можно отнести

представителей криминальных структур, уволившихся сотрудников, клиентов, хакеров, конкурентов. Для осуществления несанкционированного доступа к информации внешний нарушитель должен обладать знаниями функциональных особенностей информационной системы, знаниями и навыками применения технических средств защиты информации, данными об уязвимостях информационных систем и их технических возможностях, способах и методах реализации атак, знаниями в сфере программирования.

Доступ внешнего нарушителя к защищаемой информации осуществляется с применением телекоммуникационных сетей; аппаратных закладок; программного обеспечения, позволяющего прослушивать каналы передачи данных и модифицировать передаваемую информацию.

К внутренним нарушителям относят персонал организации; специалистов, осуществляющих различные виды работ на территории организации по договору; увольняющихся сотрудников.

Деятельность организации, препятствующая реализации угроз со стороны внутренних нарушителей, может быть осуществлена в нескольких направлениях:

– грамотный подбор и расстановка кадров для работы с информационной системой;

– контроль и разграничение доступа физических лиц к информации, к штатным средствам информационных систем и помещениям;

– контроль за порядком организации и осуществлением процесса защиты информации в организации, выполнений требований документации;

– контроль эффективности применения мер по обеспечению защиты информации.

В зависимости от прав доступа лиц к ресурсам информационных систем внутренних нарушителей принято подразделять на четыре категории [2–6].

Нарушители I категории: привилегированная категория пользователей, имеющих полномочия администратора информационной системы (системный администратор, специалист по защите информации). Знания и навыки данной категории лиц позволяют не рассматривать их в качестве нарушителей в случае ошибочных действий.

Нарушители II категории: пользователь организации, зарегистрированный в автоматизированной системе, который в силу выполнения своих должностных обязанностей может владеть следующей информацией:

– логинами-паролями всех пользователей организации;

– сведениями о структуре, функциях, механизмах и правилах функционирования технических средств защиты в организации на основании эксплуатационной документации;

– знаниями и навыками в области функционирования информационной системы в организации (функции, правила и порядок работы, формы сообщений, структура информационных потоков, сведения об уязвимостях, способы и каналы атак и т. д.).

При этом нарушители II категории имеют право доступа к штатным средствам информационной системы; программному обеспечению, позволяющему прослушивать, модифицировать каналы передачи данных и имеющиеся в свободной продаже на рынке; общедоступными компьютерными вирусами. Потенциальные нарушители II категории могут быть заинтересованы в получении персональных данных.

Нарушители III категории наряду с возможностью доступа к помещениям с техническими средствам, обеспечивающими функционирование информационной системы, характеризуются отсутствием прав доступа непосредственно к ресурсам информационной системы.

При этом нарушители данного категории владеют следующими видами информации:

– логины-пароли сотрудников организации;

– функциональные особенности применяемых в организации информационных систем;

– информация о топологии коммуникационной части подсети, протоколах и сервисах, применяемых организацией при функционировании информационной системы;

– перечень уязвимостей функционирующей в организации информационной системы, функциональные возможности технических и программных средств информационной системы;

– информация о средствах защиты, применяемых при функционировании информационной системы, принципах и алгоритмах их работы;

– информация о реальных и потенциальных угрозах и атаках на информационную систему организации.

Нарушители III категории владеют средствами доступа к определенному перечню ресурсов информационной системы:

– средствами информационной системы, оставленными без присмотра сотрудниками организации;

– средствами прослушивания каналов передачи данных и программным обеспечением для модификации данных системы, доступными для свободного приобретения;

– арсеналом доступных компьютерных вирусов.

К нарушителям IV категории относятся сотрудники организации, осуществляющие разработку и внедрение в деятельность организации программного обеспечения; техническое обслуживание, ремонт, настройку и ввод в эксплуатацию различных технических средств, функционирующих в условиях применяемой информационной системы.

Нарушители IV категории обладают следующими возможностями:

– информацией о программном обеспечении, позволяющем обрабатывать данные в информационной системе, применяемых при этом алгоритмах;

– способностью внесения ошибок и закладок, в частности, вредоносного программного обеспечения, в разрабатываемую и функционирующую информационную систему;

– данными о топологии сети, средствах обработки и защиты информации, применяемыми или потенциальными для применения в информационной системе.

Для осуществления несанкционированного доступа к информационной системе нарушитель может воспользоваться тремя видами каналов:

– визуальный, физический канал – для непосредственного доступа к системе;

– открытые каналы передачи информации ограниченного доступа;

– технические каналы утечки информации.

Порядок выполнения работы

1. Для организации, выбранной при выполнении практической работы № 4, необходимо схематично составить организационную структуру с указанием всех возможных должностей.

2. Установить квалификацию нарушителя для каждой должности, указанной в организационной структуре. Данные внести в табл. 5.1.

Таблица 5.1

Результаты определения квалификации нарушителей для организации

_____

(наименование организации)

Наименование должности сотрудника	Квалификация потенциального нарушителя			
	Категория I	Категория II	Категория III	Категория IV

3. С использованием материала теоретической части и данных табл. 5.1 необходимо дать подробное словесное описание возможностей каждой должности рассматриваемой организации как потенциального нарушителя определенной категории.

4. Сделать общий вывод по результатам выполнения практической работы.

Отчет должен содержать:

1) номер и наименование работы;
2) цель работы;
3) наименование организации и организационная структура, представленная в графической форме;
4) табл. 5.1;
5) словесное описание каждой должности (после табл. 5.1);
6) вывод о проделанной работе.

Контрольные вопросы

1. Дайте определение понятию «Нарушитель информационной безопасности». Какие категории нарушителей можно выделить?

2. Приведите классификацию нарушителей информационной безопасности в зависимости от уровня знаний и уровня возможностей.

3. Назовите причины, по которым персонал организации может выступать в качестве внутреннего нарушителя информационной безопасности.

Практическая работа № 6.
КОМПЬЮТЕРНЫЕ ВИРУСЫ И АНТИВИРУСНАЯ ЗАЩИТА

Цель работы: изучить виды и характеристику компьютерных вирусов, антивирусные средства и меры профилактики компьютера от вирусов.

Оборудование: учебный персональный компьютер.

Количество часов: 2 часа.

Общие теоретические сведения

Под компьютерным вирусом понимают разновидность программного обеспечения, которое способно внедряться в код других программ, в системные области памяти, загрузочные секторы и распространять свои копии по различным каналам связи.

Объект, в котором находится вирус, называется *зараженным объектом*. Первый компьютерный вирус, замаскированный под компьютерную игру и атаковавший компьютер Apple II, появился в 1981 г. Распространение этого вируса осуществлялось через дискету. На основании данных экспертов ежегодно количество вирусов возрастает на 15 %.

Классификация вирусов представлена на рис. 6.1 [2, 3].

Вирусы могут проникать в компьютер двумя способами: через съемные диски (гибкие и лазерные) и через компьютерные сети. При этом заражение может быть как преднамеренным, так и случайным. В качестве признаков заражения системы вирусами можно рассмотреть следующие:

– появление на компьютере сообщений, изображений, звуковых сигналов, непредусмотренных выполняемыми действиями;

– произвольный запуск или закрытие, неправильное функционирование программного обеспечения;

– частые сбои в работе компьютера;

– сбои в загрузке операционной системы;

– исчезновение и появление новых файлов и т. д.

По среде обитания

- сетевые
- файловые
- загрузочные
- файлово-загрузочные
- системные

По способу заражения

- резидентные
- нерезидентные

По деструктивным возможностям (по способам воздействия)

- безвредные
- неопасные
- опасные
- очень опасные

По особенностям алгоритма вируса

- вирусы-спутники
- простейшие вирусы
- ретро-вирусы
- репликаторные вирусы-черви
- паразитические
- студенческие
- стелс-вирусы (невидимки)
- вирусы-призраки
- макровирусы
- квазивирусные (троянские)
- логические бомбы
- мутанты

Рис. 6.1. Классификация вирусов

Порядок выполнения работы

1. Составить перечень типов файлов, подверженных и не подверженных заражению компьютерными вирусами (не менее 10 пунктов по каждой позиции), проанализировать условия и последствия такого заражения (табл. 6.1).

Таблица 6.1

Оценка возможности заражения файлов компьютерными вирусами

Типы файлов, не подвергающихся заражению компьютерными вирусами	Подвергаются заражению компьютерными вирусами			
	Типы файлов (не менее 5 наименований)	Наименование вируса (не менее 10 наименований по каждому типу файла)	Условия заражения, источники	Последствия заражения
1	2	3	4	5

2. Для каждого вируса, приведенного в табл. 6.1 (столбец 3) опишите его характеристику и особенности, подберите способы профилактики и защиты компьютера. Полученные данные внесите в табл. 6.2.

Таблица 6.2

Анализ условий профилактики и защиты от вирусов

№	Наименование вируса	Характеристика вируса	Способ профилактики	Способ защиты компьютера
1	2		3	

3. Изучите антивирусное программное обеспечение, приведите его характеристику, указав особенности, достоинства и недостатки. Данные внесите в табл. 6.3.

Таблица 6.3

Результаты анализа антивирусного программного обеспечения

№	Наименование антивирусного программного обеспечения	Характеристика			
		Особенность	Достоинства	Недостатки	Отметка о сертификации

4. Сделать общий вывод по результатам выполнения практической работы.

Отчет должен содержать:

1) номер и наименование работы;
2) цель работы;
3) табл. 6.1–6.3;
4) вывод о проделанной работе.

Контрольные вопросы

1. Что называют компьютерными вирусами?
2. Приведите классификацию компьютерных вирусов по всем возможным признакам.
3. Опишите основные этапы исторического развития компьютерных вирусов, охарактеризуйте каждый из них.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р 53114–2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – Введен в действие 01.10.2009. – М. : Стандартинформ, 2009. – 20 с.

2. Малюк А. А. Защита информации в информационном обществе. – М. : Горячая линия – Телеком, 2017. – 229 с.

3. Информационная безопасность : учеб. пособие / В. И. Лойко, В. Н. Лаптев, Г. А. Аршинов, С. В. Лаптев. – Краснодар : КубГАУ, 2020. – 332 с.

4. Гафнер В. В. Информационная безопасность : учеб. пособие в 2 ч. Ч. 1. – Екатеринбург : ГОУ ВПО УГПУ, 2009. – 155 с.

5. Груздева Л. М. Основы информационной безопасности : учеб. пособие в 2 ч. Ч. 1. – М. : Юридический институт МИИТА, 2017. – 101 с.

6. Краковский Ю. М. Методы защиты информации : учеб. пособие для вузов. – СПб. : Лань, 2021. – 236 с.

7. Об утверждении Доктрины информационной безопасности Российской Федерации [Электронный ресурс] : Указ Президента РФ от 05.12.2016 № 646. – Доступ из справ.-правовой системы «КонсультантПлюс».

8. Банк данных угроз безопасности информации [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/threat.

Приложение

СПРАВОЧНЫЕ ДАННЫЕ

Реестр угроз информационной безопасности [8]

Код угрозы	Наименование угрозы	Нарушение
УБИ.001	Угроза автоматического распространения вредоносного кода в грид-системе	Конфиденциальность, целостность, доступность
УБИ.002	Угроза агрегирования данных, передаваемых в грид-системе	Конфиденциальность
УБИ.003	Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации	Конфиденциальность, целостность
УБИ.004	Угроза аппаратного сброса пароля BIOS	Целостность
УБИ.005	Гроза внедрения вредоносного кода в BIOS	Конфиденциальность, целостность, доступность
УБИ.006	Угроза внедрения кода или данных	Конфиденциальность, целостность, доступность
УБИ.007	Угроза воздействия на программы с высокими привилегиями	Конфиденциальность, целостность
УБИ.008	Угроза восстановления и/или повторного использования аутентификационной информации	Конфиденциальность
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	Конфиденциальность, целостность, доступность
УБИ.010	Угроза выхода процесса за пределы виртуальной машины	Конфиденциальность, целостность, доступность
УБИ.011	Угроза деавторизации санкционированного клиента беспроводной сети	Доступность
УБИ.012	Угроза деструктивного изменения конфигурации / среды окружения программ	Конфиденциальность, целостность, доступность
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	Целостность
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	Доступность

Продолжение таблицы

Код угрозы	Наименование угрозы	Нарушение
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	Конфиденциальность
УБИ.016	Угроза доступа к локальным файлам сервера при помощи URL	Конфиденциальность
УБИ.017	Угроза доступа / перехвата / изменения HTTP cookies	Конфиденциальность, доступность
УБИ.018	Угроза загрузки нештатной операционной системы	Конфиденциальность, целостность, доступность
УБИ.019	Угроза заражения DNS-кеша	Конфиденциальность
УБИ.020	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	Конфиденциальность, целостность, доступность
УБИ.021	Угроза злоупотребления доверием потребителей облачных услуг	Конфиденциальность, целостность
УБИ.022	Угроза избыточного выделения оперативной памяти	Доступность
УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы	Конфиденциальность, целостность, доступность
УБИ.024	Угроза изменения режимов работы аппаратных элементов компьютера	Целостность, доступность
УБИ.025	Угроза изменения системных и глобальных переменных	Конфиденциальность, целостность, доступность
УБИ.026	Угроза искажения XML-схемы	Целостность, доступность
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Целостность
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	Конфиденциальность
УБИ.029	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	Доступность
УБИ.030	Угроза использования информации идентификации / аутентификации, заданной по умолчанию	Конфиденциальность, целостность, доступность

Продолжение таблицы

Код угрозы	Наименование угрозы	Нарушение
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	Конфиденциальность
УБИ.032	Угроза использования поддельных цифровых подписей BIOS	Целостность
УБИ.033	Угроза использования слабостей кодирования входных данных	Целостность, доступность
УБИ.034	Угроза использования слабостей протоколов сетевого / локального обмена данными	Конфиденциальность, целостность, доступность
УБИ.035	Угроза использования слабых криптографических алгоритмов BIOS	Конфиденциальность, целостность, доступность
УБИ.036	Угроза исследования механизмов работы программы	Конфиденциальность, доступность
УБИ.037	Угроза исследования приложения через отчеты об ошибках	Конфиденциальность
УБИ.038	Угроза исчерпания вычислительных ресурсов хранилища больших данных	Доступность
УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Целостность
УБИ.040	Угроза конфликта юрисдикций различных стран	Доступность
УБИ.041	Угроза межсайтового скриптинга	Конфиденциальность, целостность, доступность
УБИ.042	Угроза межсайтовой подделки запроса	Конфиденциальность, целостность, доступность
УБИ.043	Угроза нарушения доступности облачного сервера	Доступность
УБИ.044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Конфиденциальность, целостность, доступность
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	Конфиденциальность, целостность, доступность
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Конфиденциальность, доступность

Продолжение таблицы

Код угрозы	Наименование угрозы	Нарушение
УБИ.047	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Доступность
УБИ.048	Угроза нарушения технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин	Конфиденциальность, целостность, доступность
УБИ.049	Угроза нарушения целостности данных кеша	Целостность, доступность
УБИ.050	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	Целостность
УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Целостность, доступность
УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Целостность, доступность
УБИ.053	Угроза невозможности управления правами пользователей BIOS	Конфиденциальность, целостность, доступность
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Конфиденциальность, целостность, доступность
УБИ.055	Угроза незащищенного администрирования облачных услуг	Конфиденциальность, целостность, доступность
УБИ.056	Угроза некачественного переноса инфраструктуры в облако	Конфиденциальность, целостность, доступность
УБИ.057	Угроза неконтролируемого копирования данных внутри хранилища больших данных	Конфиденциальность
УБИ.058	Угроза неконтролируемого роста числа виртуальных машин	Доступность
УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Доступность
УБИ.060	Угроза неконтролируемого уничтожения информации хранилищем больших данных	Целостность
УБИ.061	Угроза некорректного задания структуры данных транзакции	Целостность, доступность

Продолжение таблицы

Код угрозы	Наименование угрозы	Нарушение
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счет плагинов браузера	Конфиденциальность
УБИ.063	Угроза некорректного использования функционала программного и аппаратного обеспечения	Конфиденциальность, целостность, доступность
УБИ.064	Угроза некорректной реализации политики лицензирования в облаке	Доступность
УБИ.065	Угроза неопределенности в распределении ответственности между ролями в облаке	Конфиденциальность, целостность, доступность
УБИ.066	Угроза неопределенности ответственности за обеспечение безопасности облака	Конфиденциальность, целостность, доступность
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Конфиденциальность
УБИ.068	Угроза неправомерного / некорректного использования интерфейса взаимодействия с приложением	Конфиденциальность, целостность, доступность
УБИ.069	Угроза неправомерных действий в каналах связи	Конфиденциальность, целостность
УБИ.070	Угроза непрерывной модернизации облачной инфраструктуры	Целостность
УБИ.071	Угроза несанкционированного восстановления удаленной защищаемой информации	Конфиденциальность
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Конфиденциальность, целостность, доступность
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Конфиденциальность, целостность, доступность
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Конфиденциальность
УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи	Конфиденциальность

Продолжение таблицы

Код угрозы	Наименование угрозы	Нарушение
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Доступность
УБИ.077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	Целостность, доступность
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Конфиденциальность, целостность, доступность
УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	Конфиденциальность, целостность, доступность
УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Конфиденциальность, целостность
УБИ.081	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	Конфиденциальность, целостность, доступность
УБИ.082	Угроза несанкционированного доступа к сегментам вычислительного поля	Конфиденциальность, целостность
УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам	Конфиденциальность, целостность, доступность
УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Конфиденциальность, целостность, доступность
УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Конфиденциальность
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Целостность, доступность
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS	Конфиденциальность, целостность, доступность
УБИ.088	Угроза несанкционированного копирования защищаемой информации	Конфиденциальность

Окончание таблицы

Код угрозы	Наименование угрозы	Нарушение
УБИ.089	Угроза несанкционированного редактирования реестра	Конфиденциальность, целостность, доступность
УБИ.090	Угроза несанкционированного создания учетной записи пользователя	Конфиденциальность, целостность
УБИ.091	Угроза несанкционированного удаления защищаемой информации	Доступность
УБИ.092	Угроза несанкционированного удаленного внеполосного доступа к аппаратным средствам	Конфиденциальность, целостность, доступность
УБИ.093	Угроза несанкционированного управления буфером	Конфиденциальность, целостность, доступность
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием	Целостность, доступность
УБИ.095	Угроза несанкционированного управления указателями	Конфиденциальность, целостность, доступность
УБИ.096	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	Конфиденциальность, целостность, доступность
УБИ.097	Угроза несогласованности правил доступа к большим данным	Конфиденциальность, доступность
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	Конфиденциальность
УБИ.099	Угроза обнаружения хостов	Конфиденциальность
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Конфиденциальность, целостность

Учебное издание

Троеглазова Анна Владимировна

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Редактор *Ю. С. Мерзликина*

Компьютерная верстка *Н. Ю. Леоновой*

Изд. лиц. ЛР № 020461 от 04.03.1997.
Подписано в печать 12.12.2022. Формат 60 × 84 1/16.
Усл. печ. л. 2,33. Тираж 70 экз. Заказ 196.
Гигиеническое заключение
№ 54.НК.05.953.П.000147.12.02. от 10.12.2002.

Редакционно-издательский отдел СГУГиТ
630108, Новосибирск, ул. Плахотного, 10.

Отпечатано в картопечатной лаборатории СГУГиТ
630108, Новосибирск, ул. Плахотного, 8.