



**НГТУ
НЭТИ**

**Факультет автоматики
и вычислительной
техники**

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

**НОВОСИБИРСК
2023**

УДК 004.3:004.056(075.8)
П 784

Коллектив авторов:

С. А. Зырянов, М. А. Кувшинов, И. А. Огнев, И. В. Никрошкин

Рецензенты:

А. В. Иванов, канд. техн. наук, зав. кафедры ЗИ НГТУ

А. Н. Фионов, д-р техн. наук, проф. кафедры ПМиК СибГУТИ

Работа подготовлена на кафедре защиты информации

П 784

Программно-аппаратные средства защиты информации : учебное пособие / С. А. Зырянов, М. А. Кувшинов, И. А. Огнев, И. В. Никрошкин. – Новосибирск : Изд-во НГТУ, 2023. – 80 с.

ISBN 978-5-7782-4905-9

В учебном пособии приведены базовые понятия информационной безопасности и теоретические сведения о средствах защиты информации. Практическая часть включает в себя примеры заданий по изучаемым темам.

Учебное пособие предназначено для студентов направлений 10.00.00 «Информационная безопасность», может быть полезно преподавателям и слушателям курсов по направлению «Информационная безопасность», а также специалистам-практикам в области защиты компьютерной информации.

УДК 004.3:004.056(075.8)

Зырянов Сергей Алексеевич
Кувшинов Максим Алексеевич
Огнев Игорь Александрович
Никрошкин Иван Владимирович

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Редактор *Е.Е. Татарникова*
Выпускающий редактор *И.П. Брованова*
Редактор *И.Е. Семенова*
Дизайн обложки *А.В. Ладыжская*
Компьютерная верстка *Л.А. Веселовская*

Налоговая льгота – Общероссийский классификатор продукции
Издание соответствует коду 95 3000 ОК 005-93 (ОКП)

Подписано в печать 21.03.2023. Формат 60 × 84 1/16. Бумага офсетная. Тираж 50 экз.
Уч.-изд. л. 4,65. Печ. л. 5,0. Изд. № 238/22. Заказ № 111. Цена договорная

Отпечатано в типографии
Новосибирского государственного технического университета
630073, г. Новосибирск, пр. К. Маркса, 20

ISBN 978-5-7782-4905-9

© Коллектив авторов, 2023
© Новосибирский государственный
технический университет, 2023

ОГЛАВЛЕНИЕ

Введение	6
1. Задача защиты информации.....	7
2. Требования законодательства РФ в сфере применения средств защиты информации.....	10
2.1. Основные нормативные акты по применению средств защиты информации.....	10
2.2. СТР-К и РД АС.....	13
2.3. Приказы ФСТЭК России и ФСБ России.....	15
2.4. Сертификация средств защиты информации ФСТЭК и ФСБ.....	16
2.4.1. Общие требования законодательства.....	16
2.4.2. Общие требования к безопасности СЗИ.....	18
3. Программно-аппаратные средства защиты информации	21
3.1. Средства защиты от несанкционированного доступа	22
3.1.1. Система идентификации и аутентификации	22
3.1.2. Системы разграничения доступа	23
3.1.3. Средства доверенной загрузки.....	25
3.1.4. Аппаратные средства аутентификации и хранения ключевой информации.....	27
3.1.5. Замкнутые программные среды.....	28
3.1.6. Подсистема регистрации и учета.....	29
3.1.7. Средства контроля съемных машинных носителей информации	31
Контрольные вопросы	31

3.2. Межсетевые экраны.....	32
3.2.1. Классические межсетевые экраны	32
3.2.2. Межсетевые экраны уровня веб-приложений	35
3.2.3. Универсальный шлюз безопасности	36
3.2.4. Межсетевые экраны нового поколения	37
Контрольные вопросы	38
3.3. Системы обнаружения вторжений	39
Контрольные вопросы	41
3.4. Средства антивирусной защиты информации.....	42
Контрольные вопросы	45
3.5. Операционные системы.....	46
Контрольные вопросы	46
3.6. Средства криптографической защиты информации и защиты электронной подписи.....	47
3.6.1. Средства криптографической защиты информации	47
3.6.2. Электронные подписи	47
3.6.3. Инфраструктура открытых ключей.....	50
Контрольные вопросы	53
3.7. Системы сбора, корреляции и обработки событий ИБ.....	53
Контрольные вопросы	57
3.8. Системы предотвращения утечек информации	57
Контрольные вопросы	58
3.9. Системы защиты сред виртуализации	59
3.9.1. Основы виртуализации.....	59
3.9.2. Защита средств виртуализации.....	61
Контрольные вопросы	62
3.10. Песочницы и honeypot.....	63
3.10.1. Песочницы	63
3.10.2. Honeypot.....	67
Контрольные вопросы	69
4. Практическая часть	70
4.1. Настройка СЗИ от несанкционированного доступа Dallas Lock	70

4.2. Работа с операционной системой Astra Linux и средством антивирусной защиты Kaspersky Endpoint Security	71
4.3. Настройка МСЭ в СЗИ от несанкционированного доступа Secret Net Studio, работа со сканером уязвимостей «Сканер-ВС»	72
4.4. Создание правил для IDS Snort.....	73
Библиографический список	75

1. ЗАДАЧА ЗАЩИТЫ ИНФОРМАЦИИ

Передовые информационные системы почти всех компаний как государственного, так и частного сектора соединены сетями (рис. 1), при этом различают соединения в пределах одной или разных организаций, а также соединения между организацией и неограниченным кругом лиц [1].

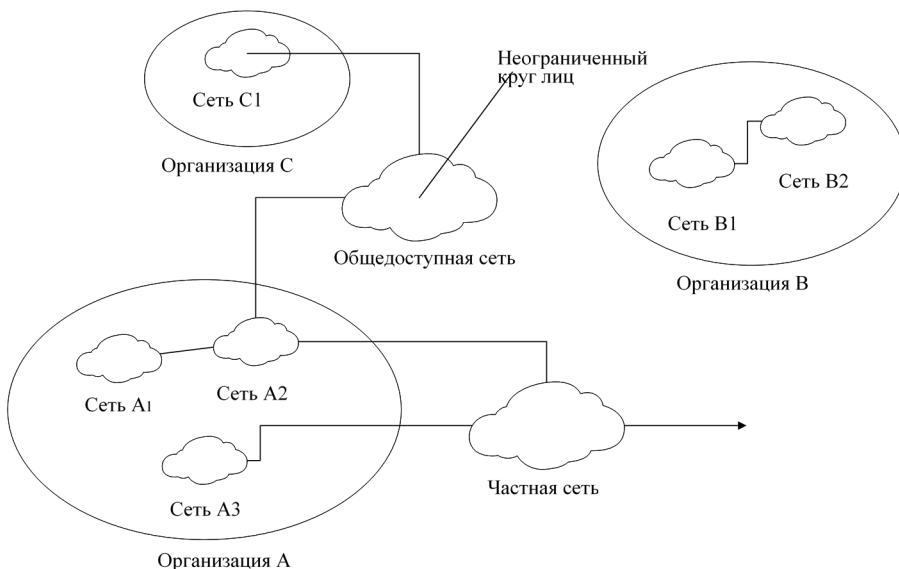


Рис. 1. Виды сетевых соединений

Стремительное развитие технологий, в том числе технологий с открытым исходным кодом, приводит к расширению экономических возможностей для компаний. Современные организации все чаще

используют новые технологии для предоставления своих услуг в режиме реального времени в сети Интернет. Немаловажным фактом является и снижение цен на передачу данных по сети Интернет благодаря услугам провайдеров. Кроме цифровизации услуг компании также широко используют новые технологии для передачи визуальной и звуковой информации, что позволяет расширять возможности удаленной работы и создавать территориально распределенные рабочие коллективы.

Такое стремительное развитие современных технологий и их широкое применение во всех сферах жизни общества приводит к расширению рисков для бизнес-процессов компаний из-за возникающих угроз информационной безопасности (ИБ). Компаниям необходимо организовывать процесс защиты информации, в том числе процесс менеджмента информационной безопасности и управление рисками информационной безопасности. Нарушение таких свойств информации, как конфиденциальность, целостность и доступность, может оказать существенное негативное влияние на непрерывность деятельности организаций. Все это приводит к тому, что компаниям необходимо поддерживать информационную безопасность на должном уровне для успешного проведения основных бизнес-процессов [1].

Возможности безопасности в виде различного рода программного обеспечения, аппаратных средств и программно-аппаратных комплексов необходимы для общей безопасности. Однако по мере того, как все больше и больше продуктов объединяются для предоставления общих решений, функциональная совместимость этих продуктов (или ее отсутствие) будет определять успех решения. Следует не только заботиться о безопасности каждого продукта (услуги), но и интегрировать возможности безопасности продукта или услуги в общее решение безопасности организации.

Защита информации – это деятельность, которая направлена на предотвращение утечки защищаемых данных, а также несанкционированных и непреднамеренных воздействий на защищаемую информацию. Цель защиты информации заключается в предотвращении ущерба владельцу, собственнику или пользователю информации.

Важнейшими задачами обеспечения информационной безопасности является защита информации от следующих угроз:

- утечек;

- непреднамеренного или преднамеренного воздействия;
- разглашения;
- несанкционированного воздействия;
- несанкционированного доступа.

Существуют два основных подхода для обеспечения информационной безопасности.

1. Фрагментарный подход. Характеризуется высокой избирательностью и высокой скоростью внедрения. Основной недостаток: медленная актуализация защиты, потому что любое изменение структуры систем или актуальных угроз приводит к снижению эффективности системы защиты информации.

2. Комплексный подход. Характеризуется охватом всей инфраструктуры компании и низкой скоростью внедрения. Этот подход объединяет разнородные методы и средства защиты и предполагает внедрение менеджмента информационной безопасности.

Соответственно для поддержания информационной безопасности в надлежащем состоянии рекомендуется применять комплексный подход к построению системы защиты.