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. Бровановa*
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

ОГЛАВЛЕНИЕ

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].

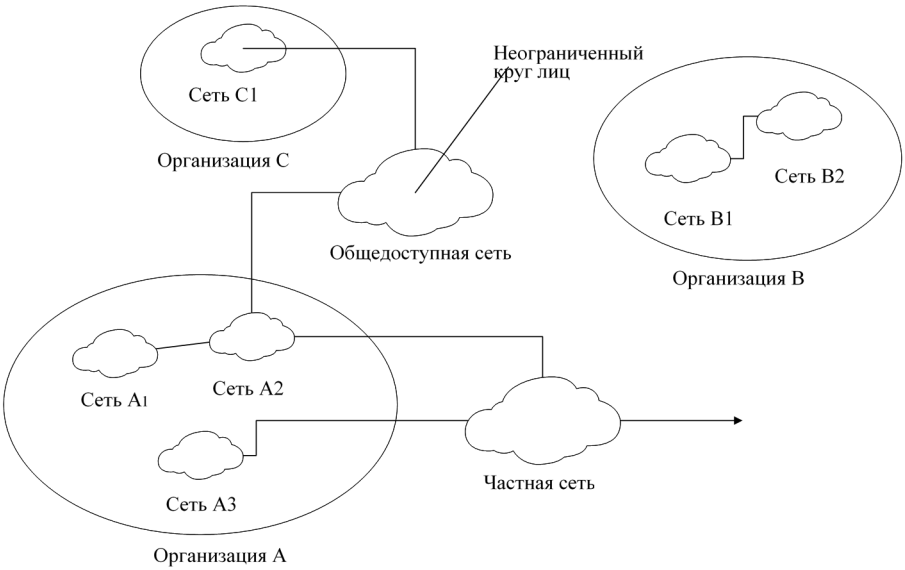

Рис. 1. Виды сетевых соединений

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.