А. В. МОРГУНОВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ



ФАКУЛЬТЕТ БИЗНЕСА

Министерство науки и высшего образования Российской Федерации
НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

А.В. МОРГУНОВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебно-методическое пособие

НОВОСИБИРСК
2019

УДК 004.056(075.8)
М 791

Рецензенты:

д-р техн. наук, профессор *Л.Г. Рогулина*
канд. экон. наук, доцент *В.И. Мамонов*

Работа подготовлена на кафедре экономической информатики
и утверждена Редакционно-издательским советом университета
в качестве учебно-методического пособия

Моргунов А.В.

М 791 Информационная безопасность: учебно-методическое пособие / А.В. Моргунов. – Новосибирск: Изд-во НГТУ, 2019. – 83 с.

ISBN 978-5-7782-3918-0

Учебно-методическое пособие включает: описание основ защиты информации, содержащейся в базах данных; информационных ресурсов; угроз утечки информации; актуальных угроз безопасности для финансово-кредитных организаций, а также авторскую методику оценки рисков нарушения информационной безопасности на предприятиях. Приводятся общие сведения об эффективных методах защиты информации баз данных.

Предназначено для студентов вузов, изучающих курс «Информационные технологии и обеспечение комплексной защиты информации», может быть полезно специалистам банковских, финансовых и инвестиционных организаций.

УДК 004.056(075.8)

ISBN 978-5-7782-3918-0

© Моргунов А.В., 2019
© Новосибирский государственный
технический университет, 2019

СПИСОК СОКРАЩЕНИЙ

АРМ – автоматизированное рабочее место;
АС – автоматизированная система;
АТС – автоматическая телефонная станция;
БД – база данных;
БС РФ – банковская сфера Российской Федерации;
ВОЛС – волоконно-оптическая линия связи;
ВТСС – вспомогательные технические средства и системы;
ДМЗ – демилитаризованная зона;
ИБ – информационная безопасность;
ИС – информационная система;
ИСПДн – информационная система обработки персональных данных;
УБПДн – угроза безопасности персональных данных;
КЗ – контролируемая зона;
КСИИ – ключевая система информационной инфраструктуры;
ЛВС – локально-вычислительная сеть;
МЭ – межсетевой экран;
НДВ – недекларированные возможности;
НСД – несанкционированный доступ;
ПМВ – программно-математическое воздействие;
ПО – программное обеспечение;
ПЭМИН – побочные электромагнитные излучения и навозки;
САЗ – система анализа защищенности;
СЗИ – средство защиты информации;
СОА – средство обнаружения компьютерных атак;
СОВ – система обнаружения вторжений;
ТЗИ – техническая защита информации;
СВР – степень возможности реализаций;
СТП – степень тяжести последствий.

ВВЕДЕНИЕ

В течение последних нескольких лет информация стала играть важнейшую роль во всех сферах человеческой жизни, что связано с постепенным становлением информационного общества. Информация, информационные технологии и появившийся рынок информационных услуг требуют пристального внимания и изучения, поскольку очевидно, что вследствие владения, использования и передачи ценной и важной информации может возникать ряд рисков, способных нанести ощутимый урон компании, государству и экономике в целом. У каждой корпорации есть секреты производства, данные об уникальных инновациях, интеллектуальной собственности, базы данных клиентов, партнеров, поставщиков, сотрудников, на которых строится весь производственный процесс, и попадание этих данных в руки конкурентам или иным недоброжелателям серьезно угрожает состоянию и функционированию компании. Предлагаемое пособие знакомит читателя с важнейшими разделами: «Основы информационной безопасности», «Актуальные угрозы утечки информации», «Основы защиты информационных ресурсов», «Определение актуальных угроз безопасности для финансово-кредитных организаций». В первом разделе приводятся основные понятия, связанные с информационной безопасностью и государственные законодательные акты, регулирующие отношения в сфере защиты информации. Во втором разделе изложена классификация угроз безопасности персональных данных, рассмотрены виды и способы угроз, возникающие по различным информационным каналам, включая социальную инженерию. В третьем и четвертом разделах делается акцент на необходимости введения основных организационных мер защиты от НСД, в том числе и для финансово-кредитных организаций, по средствам выявления актуальности угроз в ИСПДн и расчете угроз безопасности информационных систем обработки персональных данных. Для этого подробно приводится пример построения модели нарушителя информационной безопасности и демонстрируются основные уязвимости сетевых протоколов стека TCP/IP и др.

РАЗДЕЛ I

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ ТЕРМИНА «БЕЗОПАСНОСТЬ БАНКОВ ДАННЫХ»

Широкое распространение во всех отраслях автоматизированного анализа и накопления данных, в том числе и охраняемых законами Российской Федерации, увеличивает требования по безопасности таких структур.

Приведем основные определения термина «безопасность банков данных».

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Информационная безопасность Российской Федерации – это состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Также в ряде отечественных и зарубежных стандартов дается описание состояния информационной безопасности.

Целостность – свойство ИБ организации сохранять неизменность или обнаруживать факт изменения в своих информационных активах.

Доступность – свойство ИБ организации, состоящее в том, что информационные активы предоставляются авторизованному пользователю, причем в виде и месте, необходимых пользователю, и в то время, когда они ему необходимы.

Конфиденциальность – свойство ИБ организации, состоящее в том, что обработка, хранение и передача информационных активов осуществляются таким образом, что информационные активы доступны только авторизованным пользователям, объектам системы или процессам.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Вирус (*компьютерный*, *программный*) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и/или воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (*информационной системы персональных данных*) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т. п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных – это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, послужившие причиной возникновения угрозы безопасности информации.

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников, посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согла-