Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Высшая школа электроники и компьютерных наук
Кафедра «Защита информации»

РАБОТА ПРОВЕРЕНА
Рецензент, директор
ООО «Стратегия безопасности»
_____ Д.Н. Иванов
_____ 2019 г.

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2019 г.

Аттестация системы биометрической идентификации «ПАПИЛОН»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.03.2019.383.ПЗ ВКР

Консультанты

Безопасность жизнедеятельности,
к.т.н., доцент
_____ Н.В. Глотова
_____ 2019 г.

Экономическая часть,
ст. преп.
_____ С.А. Сабельников
_____ 2019 г.

Руководитель проекта,
заместитель директора ООО
«Стратегия безопасности»
_____ Е.Ю. Мищенко
_____ 2019 г.

Автор проекта,
студент группы КЭ-570
_____М.П. Медведев
_____ 2019 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2019 г.

Челябинск 2019

АННОТАЦИЯ

Медведев М.П. Аттестация системы биометрической идентификации «ПАПИЛОН» – Челябинск: ЮУрГУ, КЭ-570, 212 с., 3 ил., 18 табл., библиогр. список – 39 наим., 3 прил.

Выпускная квалификационная работа выполнена с целью участия в проведении аттестации по требованиям безопасности информации информационной системы персональных данных «АДИС-ОФБД» Производственной и IT-компании.

В разделе один проведен обзор законодательства Российской Федерации в области защиты сведений конфиденциального характера, в частности, персональных данных, а также требований законодательства Российской Федерации по защите персональных данных.

В разделе два проведены анализ исходных сведений об информационной системе персональных данных, анализ угроз безопасности персональных данных при их обработке в информационной системе, а также степень соответствия системы защиты персональных данных требованиям законодательства Российской Федерации по защите персональных данных.

В разделе три представлено теоретическое обоснование необходимости аттестации информационной системы персональных данных, а также оценена экономическая целесообразность мероприятий по аттестации.

В разделе четыре разработаны необходимые документы для проведения аттестационных испытаний информационной системы персональных данных (Программа и методики аттестационных испытаний), а также проекты документов, фиксирующих результаты проведения аттестационных испытаний по отдельным направлениям защиты персональных данных.

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

АРМ – автоматизированное рабочее место.
АС – автоматизированная система.
БДУ – Банк данных угроз (безопасности информации ФСТЭК России).
ВКР – выпускная квалификационная работа.
ВТСС – вспомогательные технические средства и системы.
ИС – информационная система.
ИСПДн – информационная система персональных данных.
НЖМД – накопитель на жестких магнитных дисках.
НСД – несанкционированный доступ.
ОТСС – основные технические средства и системы.
ПДн – персональные данные.
ПЭВМ – персональная электронно-вычислительная машина.
СрЗИ – средство защиты информации.
ФСБ – Федеральная служба безопасности.
ФСТЭК – Федеральная служба по техническому и экспортному контролю.

Автоматизированное рабочее место – программно-технический комплекс автоматизированной системы, предназначенный для автоматизации деятельности определенного вида.[1]

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.[1]

Аттестация объектов информатизации – комплекс организационно-технических мероприятий, в результате которых посредством специального документа – аттестата соответствия – подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России.[2]

Безопасность информации – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации при ее обработке техническими средствами (ГОСТ Р 50922-2006).[3]

Вспомогательные технические средства и системы – технические средства и системы, их коммуникации, не предназначенные для обработки ПДн, но размещенные в помещениях, в которых расположены ИСПДн, их технические средства.[4]

Информационная безопасность – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.[5]

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. [6]

Информационная технология – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.[6]

Информация – сведения (сообщения, данные) независимо от формы их представления.[6]

Контролируемая зона – пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств.[7]

Нормативно-методические документы – документы, определяющие порядок и правила выполнения работ, функций и операций в рабочих процессах, а также порядок и правила взаимодействия в них функционально сопряженных ролей.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.[8]

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.[9]

Организационно-распорядительные документы – документы, закрепляющие функции, задачи, цели, а также права и обязанности работников и руководителей по выполнению конкретных действий, необходимость которых возникает в операционной деятельности организации.[10]

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.[9]

Угроза безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.[4]

Уязвимость информационной системы персональных данных – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности персональных данным.[4]

ВВЕДЕНИЕ

Персональные данные граждан Российской Федерации, помимо общедоступных, – информация, установленная «Перечнем сведений конфиденциального характера» от 6 марта 1997 года №188 как сведения конфиденциального характера [11]. Факт конфиденциальности персональных данных и требование по защите персональных данных при их обработке устанавливает Федеральный закон от 27 июля 2006 года №152 «О персональных данных» [9]. Общедоступные персональные данные также необходимо защищать от угроз целостности и доступности.

Согласно положениям Федерального закона от 27 июля 2006 года №149 «Об информации, информационных технологиях и о защите информации», обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами [6].

Помимо установленных Федеральным законом №152 и подзаконными актами мер и требований по обеспечению безопасности персональных данных, требованиями подзаконных актов установлен контроль за выполнением требований по обеспечению безопасности, который, при добровольном привлечении сторонней организации, имеющей соответствующую лицензию, проводится в виде аттестации по требованиям безопасности информации. Такой контроль упрощает оператора с уполномоченными государственными органами, сводит практически к нулю вероятность обнаружения нарушений при выполнении требований законодательства, поскольку аттестат соответствия требованиям безопасности выдается организацией-третьей стороной, имеющей соответствующие лицензии, и, следовательно, осуществляющей объективный контроль.

Объектом ВКР является Производственная и IT-компания.

Предметом ВКР является ИСПДн «АДИС-ОФБД».

Объект ВКР выбрал аттестацию по требованиям безопасности информации предмета ВКР необходимой, исходя из следующих соображений:

– объект ВКР, как будет подробно описано в разделе 2, сотрудничает с ведомствами Российской Федерации и удовлетворяет потребности заказчика – ведомств в рамках расследования ими противоправных деяний. Соответственно, согласно внутренним договоренностям между объектом ВКР и МВД России, объект ВКР производит аттестацию предмета ВКР по требованиям безопасности;

– срок действия прошлого аттестата соответствия предмета ВКР требованиям безопасности информации истек;

– объект ВКР, как будет подробнее рассмотрено в разделе 2, является лицензиатом ФСТЭК России на осуществление деятельности, связанной с конфиденциальной информацией, поэтому аттестация предмета ВКР осуществляется из имиджевых соображений, оцененных руководителем объекта ВКР как необходимой для осуществления бизнеса составляющей.

Актуальность ВКР обусловлена необходимостью соблюдения требований законодательства Российской Федерации в области обработки и защиты персональных данных и аттестации ИСПДн по требованиям безопасности информации.

Целью ВКР является принятие непосредственного участия в аттестации по требованиям безопасности информации ИСПДн «АДИС-ОФБД». Аттестация объ-

ектов информатизации по требованиям безопасности информации включает в себя этапы, которые будут пройдены для достижения целей выпускной квалификационной работы:

– анализ исходных данных по объекту информатизации, обследование объекта информатизации;

– анализ системы защиты информации объекта информатизации на предмет соответствия ее требованиям нормативно-правовых актов в сфере защиты информации;

– проведение комплексных аттестационных испытаний в реальных условиях эксплуатации объекта;

– анализ результатов проведения аттестации.