

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»**

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент

_____ А.Н. Соколов
_____ 2019 г.

**Модернизация технологии обработки данных о
пользователях защищаемой информационной системы
персональных данных в муниципальном казенном учреждении
образования Свердловской области**

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.03.01.2019.188.ПЗ ВКР

Руководитель проекта,
д.п.н., профессор
_____ Л.В. Астахова
_____ 2019 г.

Автор проекта,
студент группы КЭ-454
_____ С.А. Башарин
_____ 2019 г.

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

АННОТАЦИЯ

Башарин С.А. Модернизация технологии обработки данных о пользователях защищаемой информационной системы персональных данных в муниципальном казенном учреждении образования Свердловской области – Челябинск: ЮУрГУ, КЭ-454, 155 с., 12 ил., 7 табл., библиогр. список – 17 наим., 7 прил.

Выпускная квалификационная работа выполнена с целью модернизация технологии обработки данных о пользователях защищаемой информационной системы персональных данных в муниципальном казенном учреждении образования Свердловской области.

В выпускной квалификационной работе выполняется модернизация технологии обработки данных о пользователях защищаемой информационной системы персональных данных и в ее рамках отражены все этапы аттестации системы защиты персональных данных, от сбора исходных данных до заключения о соответствии нормативным документам РФ по защите персональных данных.

В процессе выполнения квалификационной работы было проведено обследование предприятия, созданы все необходимые документы, регламентирующие порядок защиты информации, а также описывающих информационную систему персональных данных предприятия. Была создана и успешно внедрена электронная система документооборота АРМ «ЖУРНАЛ».

Изм.	Лист	№ докум.	Подпись	Дата	ЮУрГУ – 10.03.01.2019.188.ПЗ ВКР		
Разраб.		Башарин			Лит.	Лист	Листов
Пров.		Астахова				5	155
Реценз.					ЮУрГУ		
Н. Контр.		Мартынов			Кафедра ЗИ		
Утв.		Соколов					

ОГЛАВЛЕНИЕ

СПИСОК СОКРАЩЕНИЙ.....	7
ВВЕДЕНИЕ.....	10
1 ПРОВЕДЕНИЕ ОБСЛЕДОВАНИЯ МКУ ЦБ И МТО	11
1.1 Правовые основы защиты информации в МКУ ЦБ И МТО	11
1.2 Разработка технического паспорта МКУ ЦБ И МТО	12
1.3 Выявление защищаемой информации МКУ ЦБ И МТО.....	15
1.4 Описание информационной системы МКУ ЦБ И МТО	16
1.5 Выявление объектов защиты МКУ ЦБ И МТО	18
1.6 Разработка модели угроз и уязвимостей выявленных объектов защиты..	18
1.7 Расчет рисков для выявленных объектов защиты МКУ ЦБ И МТО.....	29
1.8 Разработка технического задания на систему защиту информации.....	31
1.8 Вывод.....	31
2 ТЕОРИТИЧЕСКОЕ ОБОСНОВАНИЕ ВЫБОРА СРЕДСТВ ЗАЩИТЫ	32
2.1 Обзор возможных методов устранения уязвимостей.....	32
2.2.1 Утрата носителей информации.....	32
2.2.2 Утрата и компрометация ключей и атрибутов доступа	32
2.3 Обзор научной литературы	33
2.4 Вывод.....	35
3 СОЗДАНИЕ И ВВОД В ЭКСПЛУАТАЦИЮ АРМ «ЖУРНАЛ»	36
3.1 Постановка задачи на создание АРМ «ЖУРНАЛ»	36
3.2 Создание АРМ «ЖУРНАЛ».....	37
3.3 Пример работы сотрудника с АРМ «ЖУРНАЛ».....	39
3.4 Ввод в эксплуатацию АРМ «ЖУРНАЛ»	44
3.4 Вывод.....	45
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	46
ПРИЛОЖЕНИЕ А	49
ПРИЛОЖЕНИЕ Б.....	68
ПРИЛОЖЕНИЕ В	77
ПРИЛОЖЕНИЕ Г	109
ПРИЛОЖЕНИЕ Д	135
ПРИЛОЖЕНИЕ Е.....	151
ПРИЛОЖЕНИЕ Ж.....	154

СПИСОК СОКРАЩЕНИЙ

ЗИ – защита информации;
ИБ – информационная безопасность;
ТЗ – техническое задание;
АРМ - автоматизированные рабочие места
НСД – несанкционированный доступ;
ОС – операционная система;
СЗИ – система защиты информации;
ПЭВМ – персональная электронная вычислительная машина;
ПК – персональный компьютер;
ПО – программное обеспечение;
ИТ – информационные технологии;
РФ – Российская Федерация;
ФЗ – Федеральный закон;
ФСБ – Федеральная служба безопасности;
ФСТЭК - Федеральная служба по техническому и экспортному контролю;
ПО – программное обеспечение;
ОТСС – основные технические средства и системы;
ВТСС – вспомогательные технические средства и системы;
ПП – посторонние проводники;
ИБП – источник бесперебойного питания;
USB – универсальная последовательная шина (Universal Serial Bus);
МКУ – муниципальное казенное учреждение;
ЦБ и МТО – центр бухгалтерского и материально-технического обеспечения;
Автоматизированное рабочее место – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

Информация - сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

Доступ к информации – возможность получения информации и её использования (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

Несанкционированный доступ – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

Защита информации — деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

Оператор – 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(ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств(ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных(ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

Угрозы 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, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных (ст. 19 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

Контролируемая зона – это пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Средства криптографической защиты информации – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Антивирусная защита – комплекс мер, направленных на предотвращение, обнаружение и обезвреживание действий вредоносного ПО.

Система обнаружения вторжений – программное или программно-техническое средство, реализующее функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней.

Средство анализа защищенности – программное или программно-техническое средство, реализующее функции исследования информационных систем с целью обнаружения уязвимостей, которые могут привести к нарушениям политики безопасности.

Средство доверенной загрузки – программно-техническое средство, которое осуществляет блокирование попыток несанкционированной загрузки нештатной операционной системы, контроль целостности своего программного обеспечения и среды функционирования (программной среды и аппаратных компонентов средств вычислительной техники), а также не препятствует доступу к информационным ресурсам в случае успешных контроля целостности своего программного обеспечения и среды функционирования, проверки подлинности пользователя и загружаемой операционной системы.

ВВЕДЕНИЕ

Муниципальное казенное учреждение Центр бухгалтерского и материально-технического обеспечения образовательных учреждений города Екатеринбурга Целями деятельности МКУ ЦБ и МТО образовательных учреждений города Екатеринбурга являются:

ведение квалифицированного бухгалтерского и бюджетного учета и составление соответствующей отчетности образовательных учреждений, расчета заработной платы работников, расчета по услугам, оказываемым образовательными учреждениями, учета кадровых данных и штатного расписания. Информационная система персональных данных «Парус-Бюджет 8» создана для сбора, обработки и хранения персональных данных клиентов.

Информационная система персональных данных, описанная в работе, не является реальной системой МКУ ЦБ И МТО.

Информационная система персональных данных «Парус-Бюджет 8» представляет собой физический сервер с базой персональных данных клиентов, к которому имеют доступ сотрудники отдела по работе с клиентами и администратор сервера.

В начале сотрудничества с организацией клиенты подписывают “Согласие субъекта на обработку персональных данных” разработанное специалистами по информационной безопасности. В соответствии ст. 19 Федерального закона от 27.07.2006 N 152-ФЗ (ред. 27 июля 2006 года) «О персональных данных» необходимо соблюдать меры по обеспечению безопасности персональных данных при их обработке.

Актуальность данной работы обусловлена модернизацией системы защиты информации, в том числе обновлением программного комплекса системы защиты информации. Требуется периодическая проверка эффективности системы защиты персональных данных, чтобы предотвратить возможные инциденты безопасности в организации.

Объектом выпускной квалификационной работы является МКУ ЦБ И МТО.

Предметом выпускной квалификационной работы являются информационная система персональных данных «Парус-Бюджет 8»

Целью выпускной работы является модернизация информационной системы персональных данных МКУ ЦБ И МТО.

В соответствии с целью требуется решить следующие задачи:

1. Провести обследование информационной системы персональных данных «Парус-Бюджет 8» с точки зрения защиты информации.
2. Выявить объекты защиты, защищаемую информацию и провести теоретическое обоснование выбранных средств и мер защиты.
3. Разработать план работ по модернизации информационной системы персональных данных «Парус-Бюджет 8».
4. Произвести расчет эффективности системы защиты персональных данных.