Министерство транспорта Российской Федерации

Федеральное агентство железнодорожного транспорта

ФГБОУ ВО “ДАЛЬНЕВОСТОЧНЫЙ ГОСУДАРСТВЕННЫЙ

УНИВЕРСТИТЕТ ПУТЕЙ И СООБЩЕНИЯ”

Кафедра: ”Информационные технологии

и системы”

ОТЧЕТ

по производственной практике

(по получению профессиональных умений и опыта профессиональной деятельности)

Студент гр. СО251КОБ Козеко М.В.

Руководитель

доцент, к.т.н. Гурвиц Г.А.

Хабаровск

2021

СОДЕРЖАНИЕ

[ПОЯСНИТЕЛЬНАЯ ЗАПИСКА 4](#_Toc66660612)

[ХАРАКТЕРИСТИКА 6](#_Toc66660613)

[ВВЕДЕНИЕ 7](#_Toc66660614)

[ЭТАПЫ ПРОХОЖДЕНИЯ ПРАКТИКИ 8](#_Toc66660615)

[ДНЕВНИК ПРАКТИКИ 9](#_Toc66660616)

[ЦЕЛИ И ЗАДАЧИ ИС «ЕЦОД ДВБ» 10](#_Toc66660617)

[ПАРАМЕТРЫ ИС «ЕЦОД ДВБ» 11](#_Toc66660618)

[ВИДЫ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ В «ЕЦОД ДВБ» 12](#_Toc66660619)

[ТОПОЛОГИЯ СЕТИ «ЕЦОД ДВБ» 13](#_Toc66660620)

[КОНФИГУРАЦИЯ АРМ СЕРВЕРОВ 14](#_Toc66660621)

[СПИСОК ПО НА АРМ 16](#_Toc66660622)

[СТРУКТУРА ОБРАБОТКИ ДАННЫХ И ТЕХНОЛОГИЧЕСКИЙ ПРОЦЕСС 19](#_Toc66660623)

[РЕЖИМ ОБРАБОТКИ ДАННЫХ 21](#_Toc66660624)

[СУЩЕСТВУЮЩИЕ МЕРЫ ЗАЩИТЫ 23](#_Toc66660625)

[ЗАКЛЮЧЕНИЕ 25](#_Toc66660626)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 26](#_Toc66660627)

ЗАДАНИЕ

на производственную (по получению профессиональных умений и опыта профессиональной деятельности) практику для студента специальности 10.05.03 «Информационная безопасность автоматизированных систем»

**Цель практики**: Получение профессиональных умений и опыта профессиональной деятельности по проектированию информационных систем в защищенном исполнении

**Задание на практику**: Обследование объекта информатизации - информационной системы «ЕЦОД ДВБ» ПАО Сбербанк (ЦА), блок “Технологии”, Департамент ИТ блока “Розничный бизнес”, Управление ИТ “Сберегательные продукты” и определение актуальных мер защиты информационной системы.

**Содержание практики:**

* ознакомление с деятельностью предприятия;
* прохождение инструктажа;
* ознакомление с используемым программно-техническим обеспечением корпоративной сети предприятия;
* изучение нормативной литературы по информационной безопасности;
* ознакомление с требованиями по организации защиты информации в корпоративной сети предприятия;
* изучение и овладение практическими навыками использования программно-технических средств защиты информации;
* оформление отчета.

|  |  |  |
| --- | --- | --- |
| Задание выдано студенту | Козеко М.В.\_\_\_\_\_\_  (Фамилия И.О.) | Группы СО251КОБ |
| Руководитель практики | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) | Г.А.Гурвиц |

# ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Я, Козеко Михаил Вячеславович, студент 5 курса специальности «Информационная безопасность автоматизированных систем» Дальневосточного государственного университета путей сообщения группы СО51КОБ с 08.02.21 по 07.03.21, проходил производственную практику в ПАО Сбербанк (ЦА), блок “Технологии”, Департамент ИТ блока “Розничный бизнес”, Управление ИТ “Сберегательные продукты”. На время прохождения практики основной задачей была обследование объекта информатизации – ИС «Единый центр обработки данных дальневосточного банка», далее ИС «ЕЦОД ДВБ».

При прохождении практики:

* описан объект информатизации;
* определена и описана конфигурация помещения, в которой располагается ИС.
* сделаны схемы топологии сети, а также расположения АРМов в пределах контролируемой зоны.



# ХАРАКТЕРИСТИКА

Студента 5-го курса Дальневосточного государственного университета путей сообщения института «Управления, автоматизации и телекоммуникаций» по направлению *подготовки «Информационная безопасность автоматизированных систем» Козеко Михаила Вячеславовича,* проходившему производственную практику с 08.02.2021 по 07.03.2021.

По ходу прохождения практики (по получению профессиональных умений и опыта профессиональной деятельности) ознакомился с используемым программно-техническим обеспечением корпоративной сети предприятия, изучил нормативную литературу по информационной безопасности; ознакомился с требованиями по организации защиты информации в корпоративной сети предприятия; изучил и овладел практическими навыками использования программно-технических средств защиты информации;

Все рекомендуемые нотации, наставления принимал и выполнял на должном уровне, относился к работе добросовестно. Михаил показал себя инициативным и способным действовать самостоятельно, продемонстрировал высокий уровень исполнительной дисциплины. За время практики Козеко М.В. освоил все необходимые для работы теоретические и практические навыки.

Козеко М.В. овладел следующими компетенциями:

ПК-12 Способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы;

ПК-13 Способностью участвовать в проектировании средств защиты информации автоматизированной системы;

ПК-14 Способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

ПК-25 Способностью использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований;

ПК-26 Способностью оформлять полученные рабочие результаты в виде презентаций, научно-технических отчетов, статей и докладов на научно-технических конференциях.

Достигнут 3 уровень (знать, уметь, владеть) оценки показателей владения вышеуказанными компетенциями.

Замечаний по прохождению практики нет.

В целом работу на практике можно оценить самой высокой оценкой.

Руководитель практики,

к.т.н., доцент Гурвиц Г.А.

# ВВЕДЕНИЕ

В настоящее время на предприятиях, в независимости от сферы деятельности, обрабатывается большое количество информации. Ежегодно происходит процесс развития информационных технологий по обработке и хранению информации, но в тоже время появляются новые угрозы информационной безопасности. В связи с этим разрабатываются новые и модернизируются существующий средства защиты информации.

Информацию, обрабатываемую в ИС “ЕЦОД ДВБ” ПАО Сбербанк (ЦА), блок “Технологии”, Департамент ИТ блока “Розничный бизнес”, Управление ИТ “Сберегательные продукты”, необходимо защищать в соответствии с требованиями ФСТЭК и ФСБ России.

Для достижения этих целей, руководством было принято решение разработать технический проект, на основе которого в будущем создать информационную систему в защищенном исполнении.

Для оптимизации рабочего процесса, было принято решение разбить задачу на следующие подзадачи:

* организация проекта;
* формирование требований к ИС и создаваемой в ней различных по структуре, архитектуре и применяемым информационным технологиям автоматизированных систем;
* определение общей функциональной и технической архитектур;
* выбора программного обеспечения и технической инфраструктуры;
* оформление технического проекта.

# ЭТАПЫ ПРОХОЖДЕНИЯ ПРАКТИКИ

Прохождение практики было разделено на 9 этапов:

1) **08.02.2021** Встреча с руководителем практики.

После встречи с руководителем была определена задача – провести обследование объекта информатизации – ИС «ЕЦОД ДВБ».

2) **09.02.2021-12.02.2021** Определение основных задач и целей ИС «ЕЦОД ДВБ».

Были определены задачи и цели, которые преследует ИС «ЕЦОД ДВБ».

3) **13.02.2021-14.02.2021** Определение параметров ИС «ЕЦОД ДВБ».

Были определены параметры ИС «ЕЦОД ДВБ»,

4) **15.02.2021-17.02.2021** Определение видов, обрабатываемой информации в ИС «ЕЦОД ДВБ».

Информация, которая обрабатывается в ИС «ЕЦОД ДВБ», относится к персональным данным. Также мною была проведена классификация ПДн.

5) **19.02.2021-22.02.2021** Осмотр помещений, где располагается ИС «ЕЦОД ДВБ».

Обследование АРМов, на которых ведется обработка информации. Опись АРМов.

Было выявлено, что обработка информации ведется в 1 помещении, на 7-ми АРМах и 2-х серверах.

6) **26.02.2021** Изучение ПО, используемое при обработке информации и работе с системой.

Было проведено обследование АРМов на предмет используемого ПО.

7) **27.02.2021-01.03.2021** Определение структуры обработки данных.

Были определены функции АРМов и серверов, а также составлен технологический процесс обработки информации в ИС «ЕЦОД ДВБ».

8) **02.03.2021-04.03.2021** Определение режима обработки данных.

Было проведено определение режима обработки информации в ИС «ЕЦОД ДВБ».

9) **05.03.2021-07.03.2021** Исследование существующих мер защиты.

Была проведена проверка существующих мер защиты.

# ДНЕВНИК ПРАКТИКИ

Сроки практики: 08.02.2021-07.03.2021

|  |  |
| --- | --- |
| Период | Этап |
| 08.02.2021 | Встреча с руководителем практики. |
| 09.02.2021-12.02.2021 | Определение основных задач и целей ИС «ЕЦОД ДВБ». |
| 13.02.2021-14.02.2021 | Определение параметров ИС «ЕЦОД ДВБ». |
| 15.02.2021-17.02.2021 | Определение видов, обрабатываемой информации в ИС «ЕЦОД ДВБ». |
| 19.02.2021-22.02.2021 | Осмотр помещений, где располагается ИС «ЕЦОД ДВБ». Обследование АРМов, на которых ведется обработка информации. Опись АРМов. |
| 26.02.2021 | Изучение ПО, которое используется при обработке информации. |
| 27.02.2021-01.03.2021 | Определение структуры обработки данных. |
| 02.03.2021-04.03.2021 | Определение режима обработки данных. |
| 05.03.2021-07.03.2021 | Исследование существующих мер защиты. |



Руководитель практики Гурвиц Г.А.

# ЦЕЛИ И ЗАДАЧИ ИС «ЕЦОД ДВБ»

Основные задачи ЕЦОД ДВБ:

– обеспечение контроля за наличием и движением операций внутри банковских отделений;

– обеспечение контроля за наличием и движением операций между банковскими отделениями;

– обеспечение контроля построения отчетности по операциям;

– своевременное обновление информации о счетах и операциях;

– передача сведений о счетах и клиентах в другие подразделения предприятия;

Основные цели ИС «ЕЦОД ДВБ»:

– автоматизация выполнения основных функций структурного подразделения;

– обработка информации о поступлениях и списаниях средств внутри счетов клиентов;

– передача информации о счетах между банковскими отделениями

– передача информации о клиентах между банковскими отделениями;

– хранение информации о счетах клиентов;

– хранение информации о клиентах;

– повышение эффективности управления и обеспечения обработки сведений из информационных ресурсов, необходимых для обеспечения поддержки принятия управленческих решений;

– совершенствование порядка формирования, актуализации и использования информационных ресурсов;

– организация учета в электронной форме ресурсов (и формирование механизмов их автоматизированного анализа и контроля);

– увеличение оперативности доступа к информационным ресурсам;

– повышения производительности, путем автоматизации выполнения ЕЦОД ДВБ типовых операций;

– обеспечения обработки и хранения информации ограниченного доступа в соответствии с действующим законодательством и локальными нормативными актами филиала ПАО «Сбербанк».

# ПАРАМЕТРЫ ИС «ЕЦОД ДВБ»

|  |  |
| --- | --- |
| Структура информационной системы | Распределенная информационная система |
| Архитектура информационной системы | Файл-серверная информационная система с удаленным доступом пользователей |
| Наличие (отсутствие) взаимосвязей с иными информационными системами | Имеется |
| Наличие (отсутствие) взаимосвязей (подключений) к сетям связи общего пользования | Отсутствует |
| По размещению технических средств | ТС расположены в пределах двух контролируемых зон филиала ПАО «Сбербанк». |
| Режим обработки информации в ИС | Многопользовательский |
| Режим разграничения прав доступа пользователей | Система с разграничением прав доступа пользователей |
| Режим разделения функций по управлению информационной системой | Разделенная |
| Сегментирование информационной системы | Сегментированная |
| Объем обрабатываемых персональных данных | Более 100 тысяч субъектов персональных данных |
| Категория субъектов персональных данных | Субъекты персональных данных, являющиеся и не являющиеся работниками филиала ПАО «Сбербанк». |
| Категории обрабатываемых ПДн | Иные категории персональных данных |

# ВИДЫ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ В «ЕЦОД ДВБ»

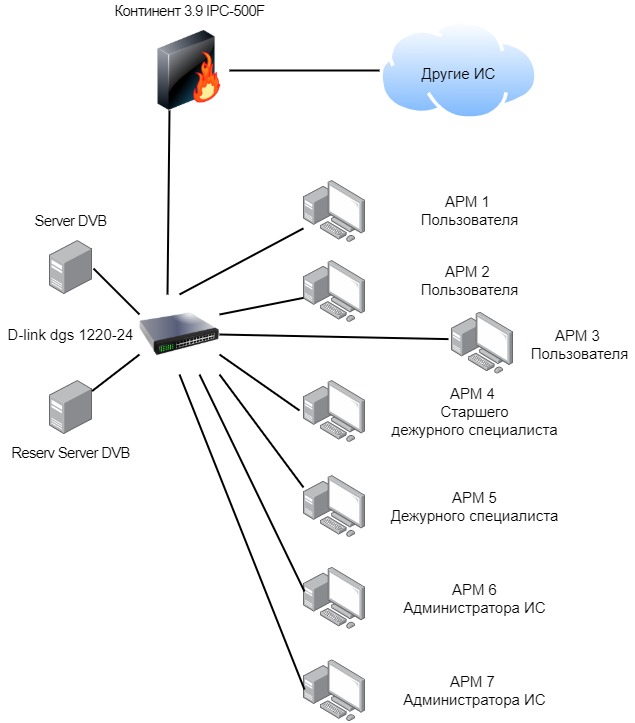
В ИС «ЕЦОД ДВБ» обрабатываются следующие виды информации:

1. Персональные данные субъектов:

* фамилия,
* имя,
* отчество,
* пол,
* дата рождения,
* место рождения,
* гражданство,
* вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
* адрес места жительства (адрес регистрации, фактического проживания);
* номер контактного телефона или сведения о других способах связи;
* семейное положение,
* состав семьи,
* сведения об образовании,
* индивидуальный номер налогоплательщика,
* данные страхового свидетельства государственного пенсионного страхования,
* расчетный счет,
* стаж работы,
* сведения о приеме на работу, перемещении по должности, увольнении, о трудовой деятельности до приема на работу,
* сведения о периодах нетрудоспособности,
* вычеты НДФЛ (вид вычета, дата начала, дата окончания, сумма);
* размер оклада, аванса, заработной платы;
* размер компенсации, основание выплаты, период, расчетные данные;
* иные персональные данные, необходимые для достижения целей структурного подразделения ПАО «Сбербанк».

2. Служебная информация.

# ТОПОЛОГИЯ СЕТИ «ЕЦОД ДВБ»



# КОНФИГУРАЦИЯ АРМ СЕРВЕРОВ

| Название АРМ | Основные технические средства и системы | |
| --- | --- | --- |
| PZ1  (АРМ 1) | Системный блок | Материнская плата: ASRock Fatal1ty Z170  Процессор: Intel Core i5-6500  Видеокарта: Intel Graphics 5000  Оперативная память: Samsung DDR4-2133 8192MB Жесткий диск: WDC WD3000HLFS-01G6U0 (500 ГБ, 10000 RPM, SATA-II); WDC WD800BB-00JHA0 (80 ГБ, 7200 RPM, Ultra­ATA/100);  Сетевая карта: Atheros AR8131 PCI-E Gigabit Ethernet Controller |
| Монитор | Acer V233H [23 LCD] |
| PZ2  (АРМ 2) | Системный блок | Материнская плата: ASRock Fatal1ty Z170  Процессор: Intel Core i5-6500  Видеокарта: Intel Graphics 5000  Оперативная память: Samsung DDR4-2133 8192MB Жесткий диск: WDC WD3000HLFS-01G6U0 (300 ГБ, 10000 RPM, SATA-II); WDC WD800BB-00JHA0 (80 ГБ, 7200 RPM, Ultra­ATA/100);  Сетевая карта: Atheros AR8131 PCI-E Gigabit Ethernet Controller |
| Монитор | Acer V233H [23 LCD] |
| Принтер | Canon LBP 2900 |
| PZ3 (АРМ 3) | Системный блок | Материнская плата: ASRock Fatal1ty Z170  Процессор: Intel Core i5-6500  Видеокарта: Intel Graphics 5000  Оперативная память: Samsung DDR4-2133 8192MB Жесткий диск: WDC WD3000HLFS-01G6U0 (300 ГБ, 10000 RPM, SATA-II); WDC WD800BB-00JHA0 (80 ГБ, 7200 RPM, Ultra­ATA/100);  Сетевая карта: Atheros AR8131 PCI-E Gigabit Ethernet Controller |
| Монитор | Acer V233H [23 LCD] |
| SDS1  (АРМ 4) | Системный блок | Материнская плата: ASRock Fatal1ty Z170  Процессор: Intel Core i5-6500  Видеокарта: Intel Graphics 5000  Оперативная память: Samsung DDR4-2133 8192MB Жесткий диск: WDC WD3000HLFS-01G6U0 (300 ГБ, 10000 RPM, SATA-II); WDC WD800BB-00JHA0 (80 ГБ, 7200 RPM, Ultra­ATA/100);  Сетевая карта: Atheros AR8131 PCI-E Gigabit Ethernet Controller |
| Монитор | EnVision LCD1971w [18,5 LCD] |
| Принтер | Kyocera FS-1035MFP KX |
| DS1  (АРМ 5) | Системный блок | Материнская плата: ASRock Fatal1ty Z170  Процессор: Intel Core i5-6500  Видеокарта: Intel Graphics 5000  Оперативная память: Samsung DDR4-2133 8192MB Жесткий диск: WDC WD3000HLFS-01G6U0 (300 ГБ, 10000 RPM, SATA-II); WDC WD800BB-00JHA0 (80 ГБ, 7200 RPM, Ultra­ATA/100);  Сетевая карта: Atheros AR8131 PCI-E Gigabit Ethernet Controller |
| Монитор | Acer V193 [19 LCD] |
| ADM1  (АРМ 6) | Системный блок | Материнская плата: ASRock Fatal1ty Z170  Процессор: Intel Core i5-6500  Видеокарта: Intel Graphics 5000  Оперативная память: Samsung DDR4-2133 8192MB Жесткий диск: WDC WD3000HLFS-01G6U0 (300 ГБ, 10000 RPM, SATA-II); WDC WD800BB-00JHA0 (80 ГБ, 7200 RPM, Ultra­ATA/100);  Сетевая карта: Atheros AR8131 PCI-E Gigabit Ethernet Controller |
| Монитор | Acer V233H [23 LCD] |
| Принтер | Samsung ML-1660 |
| ADM2  (АРМ 7) | Системный блок | Материнская плата: ASRock Fatal1ty Z170  Процессор: Intel Core i5-6500  Видеокарта: Intel Graphics 5000  Оперативная память: Samsung DDR4-2133 8192MB Жесткий диск: WDC WD3000HLFS-01G6U0 (300 ГБ, 10000 RPM, SATA-II); WDC WD800BB-00JHA0 (80 ГБ, 7200 RPM, Ultra­ATA/100);  Сетевая карта: Atheros AR8131 PCI-E Gigabit Ethernet Controller |
| Монитор | Acer V233H [23 LCD] |
| SERVER DVB | Системный блок | Материнская плата:  Single s1151,  Процессор: CPU Intel Xeon E3-1230v6, 3.50GHz, 4C/8T 8M, 72W  Оперативная память: 64Gb(4x16) DDR4 2400  ECC  Жесткие диски: HDD  2х 20Tb, SATA3, 6Gbi/s, 7.2K, 128Mb |
| Монитор | Acer AL1717 [17 LCD] |
| RESERV SERVER DVB | Системный блок | Материнская плата:  Single s1151,  Процессор: CPU Intel Xeon E3-1230v6, 3.50GHz, 4C/8T 8M, 72W  Оперативная память: 64Gb(4x16) DDR4 2400  ECC  Жесткие диски: HDD  2х 20Tb, SATA3, 6Gbi/s, 7.2K, 128Mb |
| Монитор | Acer AL1717 [17 LCD] |

# СПИСОК ПО НА АРМ

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование АРМ | Наименование программных средств | Тип ПО |
| 1 | PZ1  (АРМ 1) | Браузер Edge | Специализиро ванное ПО |
| Браузер Yandex | Специализиро­ванное ПО |
| Браузер Google | Специализиро­ванное ПО |
| Microsoft Office Профессиональный плюс 2010 | Офисное ПО |
| SbisCryptoPlugin | Специализиро­ванное ПО |
| Агент администрирования Kaspersky Security Center | СЗИ |
| Программное изделие «Kaspersky Endpoint Security для Windows (версия 11.3.0.773)» | СЗИ |
| WinRAR | Прикладное ПО |
| Cisco anyconnect | Специализиро­ванное ПО |
| КриптоПро CSP версия 3.6 | СКЗИ |
| Компонент формирования эл. подписи | Специализиро­ванное ПО |
| Печать НД с PDF417 3.0.32 (пакет) | Специализиро­ванное ПО |
| Браузер Edge | Специализиро ванное ПО |
| Браузер Yandex | Специализиро­ванное ПО |
| Браузер Google | Специализиро­ванное ПО |
| 2 | PZ2  (АРМ 2) | Браузер Edge | Специализиро ванное ПО |
| Браузер Yandex | Специализиро­ванное ПО |
| Браузер Google | Специализиро­ванное ПО |
| WinRAR | Прикладное ПО |
| Агент администрирования Kaspersky Security Center | СЗИ |
| Программное изделие «Kaspersky Endpoint Security для Windows (версия 11.3.0.773)» | СЗИ |
| Cisco anyconnect | Специализиро­ванное ПО |
| КриптоПро CSP версия 3.6 | СКЗИ |
| Печать НД с PDF417 3.0.29 (пакет) | Специализиро­ванное ПО |
| 3 | PZ3 (АРМ 3) | Браузер Edge | Специализиро ванное ПО |
| Браузер Yandex | Специализиро­ванное ПО |
| Браузер Google | Специализиро­ванное ПО |
| WinRAR | Прикладное ПО |
| Агент администрирования Kaspersky Security Center | СЗИ |
| Программное изделие «Kaspersky Endpoint Security для Windows (версия 11.3.0.773)» | СЗИ |
| Cisco anyconnect | Специализиро­ванное ПО |
| КриптоПро CSP версия 3.6 | СКЗИ |
| Печать НД с PDF417 3.0.29 (пакет) | Специализиро­ванное ПО |
| Microsoft Windows 10 Professional | Операционная  система |
| Microsoft Office Enterprise 2010 | Офисное ПО |
| 4 | SDS1  (АРМ 4) | Браузер Edge | Специализиро ванное ПО |
| Браузер Yandex | Специализиро­ванное ПО |
| Браузер Google | Специализиро­ванное ПО |
| SbisCryptoPlugin | Специализиро­ванное ПО |
| WinRAR | Прикладное ПО |
| Агент администрирования Kaspersky Security Center | СЗИ |
| Программное изделие «Kaspersky Endpoint Security для Windows (версия 11.3.0.773)» | СЗИ |
| КриптоПро CSP версия 3.6 | СКЗИ |
| СБиС++ сборки 2.4 для установки на сетевые рабочие места | Специализиро­ванное ПО |
| СБиС++ Бухгалтерия (многопользовательская установка) сборки 2.4.187 от 11.01.2014 2.4.187 от 11.01.2014 | Специализиро­ванное ПО |
| 5 | DS1  (АРМ 5) | Браузер Edge | Специализиро ванное ПО |
| Браузер Yandex | Специализиро­ванное ПО |
| Браузер Google | Специализиро­ванное ПО |
| WinRAR | Прикладное ПО |
| Агент администрирования Kaspersky Security Center | СЗИ |
| Программное изделие «Kaspersky Endpoint Security для Windows (версия 11.3.0.773)» | СЗИ |
| КриптоПро CSP версия 3.6 | СКЗИ |
| СБиС++ сборки 2.4 для установки на сетевые рабочие места | Специализиро­ванное ПО |
| 6 | ADM1  (АРМ 6) | Браузер Edge | Специализиро ванное ПО |
| Браузер Yandex | Специализиро­ванное ПО |
| Браузер Google | Специализиро­ванное ПО |
| ABBYY Lingvo x5 | Специализиро­ванное ПО |
| Microsoft Office Enterprise 2010 | Офисное ПО |
| WinRAR | Прикладное ПО |
| Агент администрирования Kaspersky Security Center | СЗИ |
| Декларация 2012 | Специализиро­ванное ПО |
| КриптоПро CSP версия 3.6 | СКЗИ |
| Программное изделие «Kaspersky Endpoint Security для Windows (версия 11.3.0.773)» | СЗИ |
| Печать НД с PDF417 3.0.29 (пакет) | Специализиро­ванное ПО |
| 7 | ADM2  (АРМ 7) | Microsoft Windows 10 Professional | Операционная  система |
| Putty | Специализиро­ванное ПО |
| Microsoft Office Enterprise 2010 | Офисное ПО |
| WinRAR | Прикладное ПО |
| Агент администрирования Kaspersky Security Center | СЗИ |
| Программное изделие «Kaspersky Endpoint Security для Windows (версия 11.3.0.773)» | СЗИ |
| 8 | SERVER DVB | Браузер Edge | Специализиро ванное ПО |
| Браузер Yandex | Специализиро­ванное ПО |
| Браузер Google | Специализиро­ванное ПО |
| WinRAR | Прикладное ПО |
| Плагин управления Kaspersky Endpoint Security 10 для Windows | СЗИ |
| Плагин управления Антивирусом Касперского | СЗИ |
| ПО резервного копирования Acronis Backup & Recovery | Специализированное ПО |  |
| СБиС++ сборки 2.4 для установки на сетевые рабочие места | Специализиро­ванное ПО |
| Сервер администрирования Kaspersky Security Center | СЗИ |
|  |  | Браузер Edge | Специализиро ванное ПО |
|  | RESERV  SERVER DVB | Браузер Yandex | Специализиро­ванное ПО |
| 9 |  | Браузер Google | Специализиро­ванное ПО |
|  |  | WinRAR | Прикладное ПО |
|  |  | Плагин управления Kaspersky Endpoint Security 10 для Windows | СЗИ |
|  |  | Плагин управления Антивирусом Касперского | СЗИ |
|  |  | СБиС++ сборки 2.4 для установки на сетевые рабочие места | Специализиро­ванное ПО |
|  |  | Сервер администрирования Kaspersky Security Center | СЗИ |
|  |  | Агент резервирования Acronis Backup & Recovery 10 | Специализированное ПО |

# СТРУКТУРА ОБРАБОТКИ ДАННЫХ И ТЕХНОЛОГИЧЕСКИЙ ПРОЦЕСС

ИС «ЕЦОД ДВБ» объединяет 7 АРМ пользователей:

* три АРМ пользователей отдела;
* одно АРМ старшего дежурного специалиста;
* одно АРМ дежурного специалиста;
* два АРМ администратора ИС;

А также два сервера для выполнения задач ЕЦОД, из которых:

* физический сервер «RESERV SERVER DVB», предназначенный для резервирования сервера ЕЦОД;
* физический сервер «SERVER DVB», предназначенных для решения задач ЕЦОД;

Технологический процесс обработки информации в ИС «ЕЦОД ДВБ» включает в себя:

* загрузку операционной системы;
* проведение антивирусного контроля;
* запуск офисных приложений и специального ПО;
* разработка текстовых документов;
* формирование и печать документов.

Технология обработки информации в филиале «Сбербанк» не предполагает передачу и хранение информации с помощью съемных машинных носителей информации.

Антивирусная защита осуществляется с применением разрешенных программных средств, в соответствии с инструкцией по проведению антивирусного контроля в ИС.

Используемые антивирусные средства указываются в Перечне разрешенного к использованию в ИС программного обеспечения.

Печать документов осуществляется на печатающем устройстве (принтере) ИС.

Регистрация листов, используемых для распечатки конфиденциальных документов, осуществляется пользователями в соответствии с требованиями инструкции по обращению с носителями информации ограниченного доступа.

Пользователь, распечатавший конфиденциальный документ, регистрирует его у сотрудника, ответственного за ведение конфиденциального делопроизводства.

Оформление, распечатка, учёт и уничтожение документов производится в соответствии с требованиями настоящего технологического процесса, инструкцией по работе пользователя в ИС, инструкции по обращению с носителями КИ.

Контроль за распечаткой документов возлагается на ответственного за эксплуатацию объекта информатизации.

Целостность и доступность информации в ИС поддерживается путем резервирования аппаратных средств, использования надежных элементов ИС и отказоустойчивых систем.

Для повышения эффективности работы сотрудников Бухгалтерии, их оперативного взаимодействия с другими структурными подразделениями филиала «Сбербанк» в ИС применяется система электронного документооборота.

Устройствами ввода информации в ИС являются клавиатуры, сканеры, МФУ.

Устройствами вывода – мониторы, принтеры, МФУ.

Субъектами доступа в информационной системе являются работники филиала «Сбербанк», имеющие право обрабатывать информацию, а также лица, обладающие правами контроля за режимом обеспечения безопасности информации в филиале «Сбербанк», в соответствии с Правилами разграничения прав доступа и Разрешительной системой доступа к информационным ресурсам.

# РЕЖИМ ОБРАБОТКИ ДАННЫХ

В ИС «ЕЦОД ДВБ» обработка информации ограниченного доступа осуществляется в многопользовательском режиме с разграничением прав доступа.

Принцип разграничения прав доступа пользователей – ролевой, дискреционный. Все пользователи в ИС имеют собственные роли и, в соответствии с ролью, права доступа и разрешенные действия. Сотрудники, допущенные к обработке информации ограниченного доступа, указаны в организационно-распорядительных документах для ИС филиала «Сбербанк».

В таблице представлен список ролей в виде матрицы доступа ИС «ЕЦОД ДВБ».

| **Привилегии и права, ресурс** | **Администратор ИС (Дежурный ИС)** | **Администратор ИБ** | **Пользователи ИС** |
| --- | --- | --- | --- |
| Привилегии и права | | | |
| Изменение настроек политик ветки домена «Сбербанк» | + | - | - |
| Запрет изменения системных файлов на серверах БД | - | - | + |
| Вывод защищаемой информации на принтер | + | + | + |
| Загрузка ПЭВМ с внешних носителей (доступ к BIOS) | + | - | - |
| Запрет изменения системных файлов АРМ пользователей | - | + | + |
| Изменение личного пароля пользователя | + | - | - |
| Работа с системным журналом ОС | + | + | - |
| Возможность создания личных ресурсов на локальных АРМ | + | + | + |
| Возможность создания ресурсов на серверах БД | + | - | - |
| Восстановление информационных ресурсов серверов БД | + | - | - |
| Работа с системным журналом СЗИ | - | + | - |
| Установка, настройка, сопровождение СЗИ | - | + | - |
| Ресурс | | | |
| Доступ к общим сетевым ресурсам на АРМ пользователей | RWA | RWA | RWA |
| Доступ к локальным папкам пользователей | RWAXD | - | RWAXD |
| Центральные БД ИС | RWAXD | - | RWXD |
| Доступ к средствам управления БД | RWAXD | - | - |
| Доступ к средствам управления СЗИ |  | RWAXDS |  |

* R - разрешение на открытие файлов только для чтения;
* W - разрешение на открытие файлов для записи;
* A - разрешение на создание файлов на диске/создание таблиц в БД;
* D - разрешение на удаление файлов/записи в БД;
* Х - разрешение на запуск программ;
* S - разрешение на настройку средств защиты.

# СУЩЕСТВУЮЩИЕ МЕРЫ ЗАЩИТЫ

Пропуск работников и посетителей на объект осуществляется в соответствии с Инструкцией по организации пропускного и внутриобъектового режима в филиале «Сбербанк» по пропускам, служебным удостоверениям и спискам.

Центральный вход в здание оборудован двойной запирающейся дверью.

Запасной вход оборудован железной запирающейся дверью, выходящею на охраняемую территорию.

Доступ в здание возможен только через входной пропускной пункт. По периметру территории установлены система освещения и видеонаблюдения.

Административное здание оснащено охранно – пожарной сигнализацией.

***Характеристика поста:***

Постов охраны – 1 (один).

Количество охранников на посту - 2 (два).

Режим охраны – круглосуточный.

Продолжительность охраны 1 охранником – 24 часа (нахождение на посту более 24 часов категорически запрещено).

В ИС «ЕЦОД ДВБ» предусмотрено резервное копирование данных, резервные копии файлов хранятся на физическом сервере ЕЦОД.

Результаты обследования показали, что защита от несанкционированного доступа нарушителей к информации, содержащейся в информационной системе «ЕЦОД ДВБ», не соответствует нормативным документам ФСТЭК и ФСБ России.

Антивирусная защита АРМ, входящих в состав ИС, обеспечивается средством антивирусной защиты Программное изделие «Kaspersky Endpoint Security для Windows (версия 11.3.0.773)».

Защита информации ограниченного доступа, передаваемой в иные ИС сторонних организаций, обеспечивается средством криптографической защиты «КриптоПро CSP».

В ИС «ЕЦОД ДВБ» введены следующие организационные и физические меры защиты:

* разработаны документы, определяющие политику в отношении обработки информации ограниченного доступа;
* организованы контролируемые зоны филиала «Сбербанк»;
* реализован контроль доступа в помещение, где расположены элементы ИС;
* установлена охранная сигнализация;
* установлена пожарная сигнализация;
* входные двери кабинетов, в которых осуществляется обработка информации ограниченного доступа, в нерабочее время и в случае отсутствия в них сотрудников закрываются на ключ;

окна кабинетов, в которых осуществляется обработка информации ограниченного доступа, оборудованы жалюзи и решетками.

# ЗАКЛЮЧЕНИЕ

В результате прохождения производственной практики были получены профессиональные умения и опыт по проектированию информационных систем в защищенном исполнении. В результате ознакомления с рядом нормативно-правовых актов, государственных стандартов и методических рекомендаций были приобретены теоретические навыки, необходимые при разработке информационной системы. Конечным результатом прохождения данной практики является готовый документ, который является начальным для разработки технического проекта автоматизированной системы в защищенном исполнении.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: федер. закон от от 27.07.2006 № 149-ФЗ, ред. от 18.03.2019 – Режим доступа: http://www.consultant.ru/document/cons\_doc\_LAW\_61798/, свободный. – Загл. с экрана.
2. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Электронный ресурс]: приказ ФСТЭК РФ от 11.02.2013 №17 – Режим доступа: http://fstec.ru/component/attachments/download/567, свободный. – Загл. с экрана.
3. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: постановление Правительства РФ от 01.11.2012 № 1119 – Режим доступа: http://www.consultant.ru/document/cons\_doc\_LAW\_137356/, свободный. – Загл. с экрана.
4. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: приказ ФСТЭК РФ от 18.02.2013 №21 – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21, свободный. – Загл. с экрана.
5. Защита информации. Основные термины и определения: ГОСТ Р 50922-2006 [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/gost-r-50922-2006, свободный. – Загл. с экрана.
6. О персональных данных [Электронный ресурс]: федер. закон от от 27.07.2006 № 152-ФЗ, ред. от 31.12.2017 – Режим доступа: http://www.consultant.ru/document/cons\_doc\_LAW\_61801, свободный. – Загл. с экрана.