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 Ильченко М.А.

Руководитель

доцент кафедры ИТиС,

к.т.н Антонов Р.А.

Хабаровск

2021

# СОДЕРЖАНИЕ

[СОДЕРЖАНИЕ 2](#_Toc68537317)

[ЗАДАНИЕ 3](#_Toc68537318)

[ПОЯСНИТЕЛЬНАЯ ЗАПИСКА 4](#_Toc68537319)

[ХАРАКТЕРИСТИКА 6](#_Toc68537320)

[ВВЕДЕНИЕ 7](#_Toc68537321)

[ЭТАПЫ ПРОХОЖДЕНИЯ ПРАКТИКИ 8](#_Toc68537322)

[ДНЕВНИК ПРАКТИКИ 9](#_Toc68537323)

[ЦЕЛИ И ЗАДАЧИ ИС «ЕФС ДВБ» 10](#_Toc68537324)

[ПАРАМЕТРЫ ИС «ЕФС ДВБ» 11](#_Toc68537325)

[ВИДЫ ИНФОРМАЦИИ ОБРАБАТЫВАЕМОЙ В ИС «ЕФС ДВБ» 12](#_Toc68537326)

[ТОПОЛОГИЯ «ЕФС ДВБ» 13](#_Toc68537327)

[КОНФИГУРАЦИЯ АРМОВ И СЕРВЕРОВ 14](#_Toc68537328)

[СПИСОК ПО УСТАНОВЛЕННОГО НА АРМ 16](#_Toc68537329)

[СТРУКТУРА ОБРАБОТКИ ДАННЫХ И ТЕХНОЛОГИЧЕСКИЙ ПРОЦЕСС 18](#_Toc68537330)

[РЕЖИМ ОБРАБОТКИ ДАННЫХ 20](#_Toc68537331)

[СУЩЕСТВУЮЩИЕ МЕРЫ ЗАЩИТЫ 22](#_Toc68537332)

[ЗАКЛЮЧЕНИЕ 24](#_Toc68537333)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 25](#_Toc68537334)

# 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 «ЕФС 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.

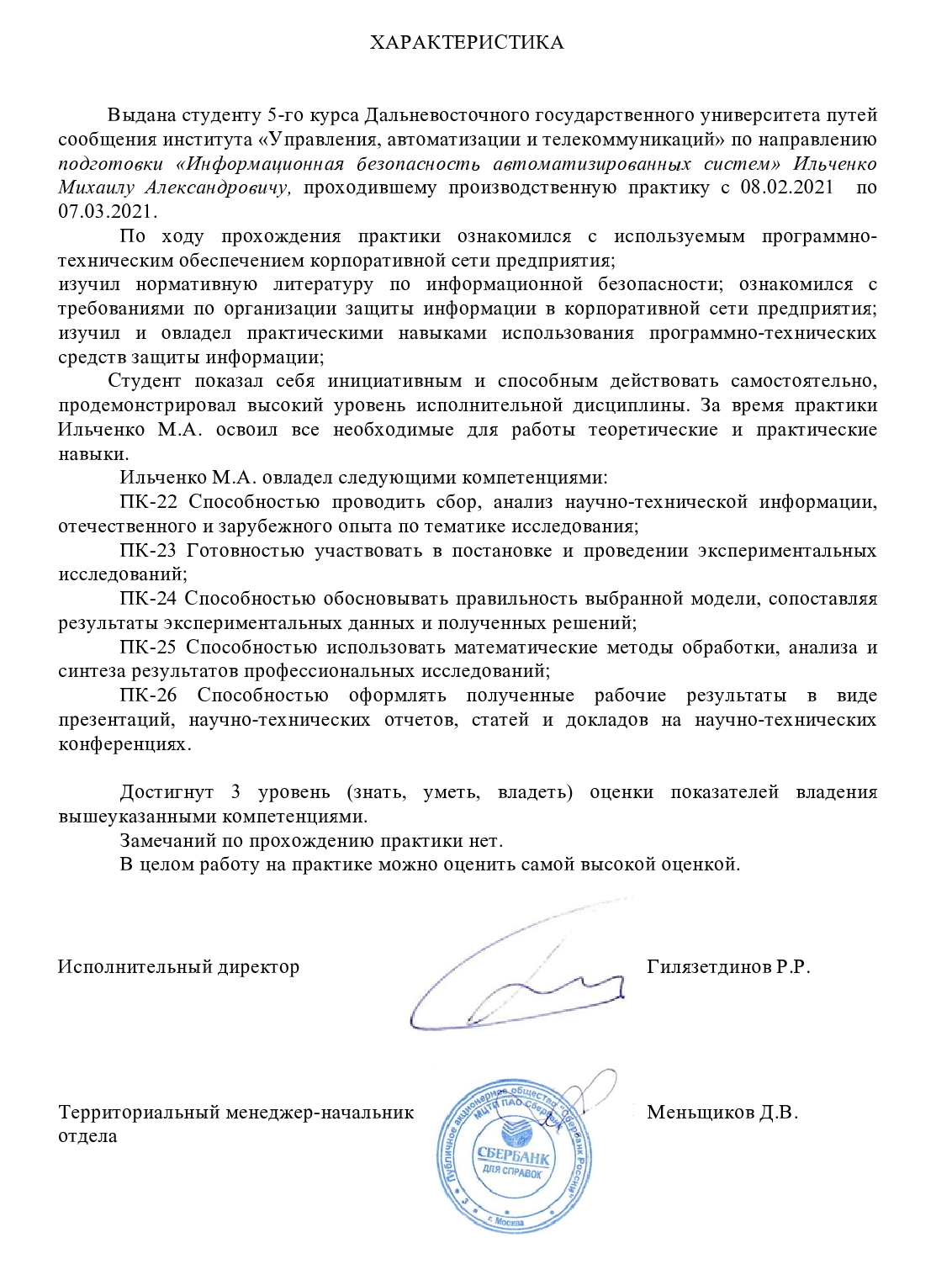
|  |  |  |
| --- | --- | --- |
| Задание выдано студенту | Ильченко М.А.\_\_\_\_\_\_  (Фамилия И.О.) | Группы СО251КОБ |
| Руководитель практики | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) | Р.А. Антонов |

# ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Я, Ильченко Михаил Александрович, 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 «Единая фронтальная система дальневосточного банка», далее ИС «ЕФС ДВБ».

При прохождении практики:

* описан объект информатизации;
* определена и описана конфигурация помещения, в которой располагается ИС.
* сделаны схемы топологии сети, а также расположения АРМ 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» Ильченко Михаила Александровича, 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 Ильченко М.А. освоил все необходимые для работы теоретические и практические навыки.

Замечаний по прохождению практики нет.

В целом работу на практике оцениваю “отлично”.

Руководитель практики,

доцент кафедры ИТиС, к.т.н Антонов Р.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 существующие средства защиты информации.

Для защиты информации в ИС “ЕФС ДВБ” ПАО Сбербанк (ЦА), блок “Технологии”, Департамент ИТ блока “Розничный бизнес”, Управление ИТ “Сберегательные продукты” 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 «ЕФС ДВБ».

2) 09.02.2021-11.02.2021 Определение основных задач и целей ИС «ЕФС ДВБ».

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

3) 12.02.2021-13.02.2021 Определение параметров ИС «ЕФС ДВБ».

Были определены параметры ИС «ЕФС ДВБ»,

4) 14.02.2021-16.02.2021 Определение видов, обрабатываемой информации в ИС «ЕФС ДВБ».

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

5) 17.02.2021-20.02.2021 Осмотр помещений, где располагается ИС «ЕФС ДВБ».

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

Было выявлено, что обработка информации ведется в 1 помещении, на 5-ти АРМах и 2-ом серверах.

6) 21.02.2021-24.02.2021 Изучение ПО, используемого при обработке информации и работе с системой.

Было проведено обследование АРМов на предмет используемого ПО.

7) 25.02.2021-01.03.2021 Определение структуры обработки данных.

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

8) 02.03.2021-04.03.2021 Определение режима обработки данных.

Было проведено определение режима обработки информации в ИС «ЕФС 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. |
| 09.02.2021-11.02.2021 | Определение основных задач и целей ИС «ЕФС ДВБ». |
| 12.02.2021-13.02.2021 | Определение параметров ИС «ЕФС ДВБ». |
| 14.02.2021-16.02.2021 | Определение видов, обрабатываемой информации в ИС «ЕФС ДВБ». |
| 17.02.2021-20.02.2021 | Осмотр помещений, где располагается ИС «ЕФС ДВБ». Обследование АРМов, на которых ведется обработка информации. Опись всех АРМ. |
| 21.02.2021-24.02.2021 | Изучение ПО, которое используется при обработке информации. |
| 25.02.2021-01.03.2021 | 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 Антонов Р.А.

# ЦЕЛИ И ЗАДАЧИ ИС «ЕФС ДВБ»

Основные задачи ЕФС ДВБ:

– обеспечение мониторинга работоспособности сопровождаемых серверов и сервисов банка;

– совершенствование текущей системы мониторинга;

– оповещение компетентных органов банка о произошедших отклонениях и инцидентах;

– обеспечение плановых внедрений ПО на сопровождаемые сервисы.

Основные цели ИС «ЕФС ДВБ»:

– реагирование на уведомления об отклонениях в работе подсистем ИС ЕФС ДВБ;

– анализ инфраструктурных метрик серверов приложений;

– информирование коллег о текущих отклонениях и инцидентах;

– обработка информации о произошедших отклонениях, инцидентах, обновлениях ПО;

– инициирование собрания оперативных конференций для решения возникающих инцидентов;

– передача технологической информации об ИС ЕФС ДВБ коллегам смежных и вышестоящих направлений;

– проведение плановых работ по внедрению новых версий ПО на сопровождаемые сервисы;

– тестирование внедряемых версий ПО на сопровождаемые сервисы;

– хранение информации о счетах клиентов;

– хранение информации о клиентах;

– обработка информации об операциях со счетами клиентов;

– оперативное решение задач, возникших в ходе эксплуатации ИС ЕФС ДВБ коллегами нижестоящих направлений;

– повышения производительности, путем автоматизации выполнения ЕФС ДВБ типовых операций.

# ПАРАМЕТРЫ ИС «ЕФС 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 ИС «ЕФС ДВБ»

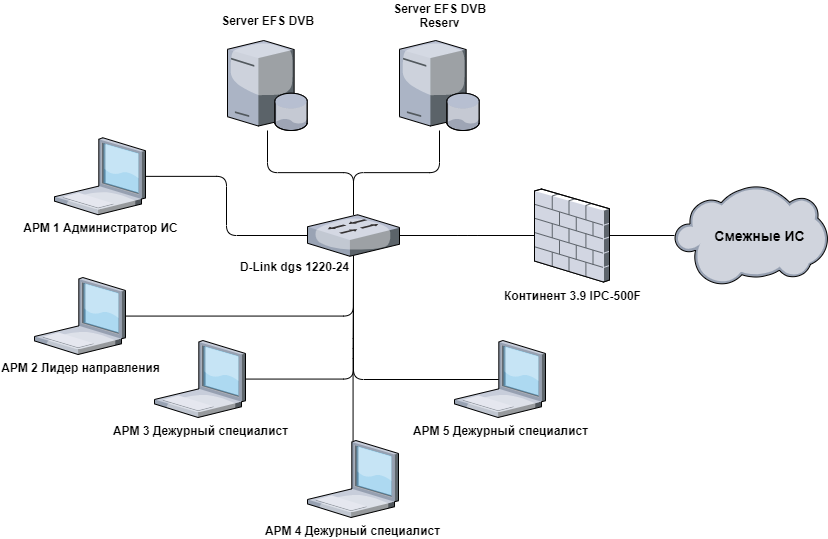
В ИС «ЕФС ДВБ» обрабатываются следующие виды информации:

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;
* индивидуальный номер налогоплательщика,
* данные страхового свидетельства государственного пенсионного страхования,
* расчетный счет,
* сведения о приеме на работу, перемещении по должности, увольнении, о трудовой деятельности до приема на работу,
* вычеты НДФЛ (вид вычета, дата начала, дата окончания, сумма);
* иные персональные данные, необходимые для достижения целей структурного подразделения ПАО «Сбербанк».

2. Служебная технологическая информация.

# ТОПОЛОГИЯ «ЕФС ДВБ»



# КОНФИГУРАЦИЯ АРМ И СЕРВЕРОВ

| Название АРМ | Основные технические средства и системы | |
| --- | --- | --- |
| 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] |
| 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 |
| 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] |
| 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 |
| 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] |
| Монитор | Acer V233H [23 LCD] |
| Server EFS 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] |
| Server EFS DVB Reserv | 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 УСТАНОВЛЕННОГО НА АРМ

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование АРМ | Наименование программных средств | Тип ПО |
| 1 | АРМ 1 | Браузер Yandex | Специализиро­ванное ПО |
| Браузер Google Chrome | Специализиро­ванное ПО |
| Microsoft Office Профессиональный 2010 | Офисное ПО |
| Kaspersky Endpoint Security для Windows | СЗИ |
| WinRAR | Прикладное ПО |
| Cisco anyconnect | Специализиро­ванное ПО |
| КриптоПро CSP | СКЗИ |
| 2 | АРМ 2 | Браузер Yandex | Специализиро­ванное ПО |
| Браузер Google Chrome | Специализиро­ванное ПО |
| Microsoft Office Профессиональный 2010 | Офисное ПО |
| Kaspersky Endpoint Security для Windows | СЗИ |
| WinRAR | Прикладное ПО |
| Cisco anyconnect | Специализиро­ванное ПО |
| КриптоПро CSP | СКЗИ |
| 3 | АРМ 3 | Браузер Yandex | Специализиро­ванное ПО |
| Браузер Google Chrome | Специализиро­ванное ПО |
| Microsoft Office Профессиональный 2010 | Офисное ПО |
| Kaspersky Endpoint Security для Windows | СЗИ |
| WinRAR | Прикладное ПО |
| Cisco anyconnect | Специализиро­ванное ПО |
| КриптоПро CSP | СКЗИ |
| 4 | АРМ 4 | Браузер Yandex | Специализиро­ванное ПО |
| Браузер Google Chrome | Специализиро­ванное ПО |
| Microsoft Office Профессиональный 2010 | Офисное ПО |
| Kaspersky Endpoint Security для Windows | СЗИ |
| WinRAR | Прикладное ПО |
| Cisco anyconnect | Специализиро­ванное ПО |
| КриптоПро CSP | СКЗИ |
| 5 | АРМ 5 | Браузер Yandex | Специализиро­ванное ПО |
| Браузер Google Chrome | Специализиро­ванное ПО |
| Microsoft Office Профессиональный 2010 | Офисное ПО |
| Kaspersky Endpoint Security для Windows | СЗИ |
| WinRAR | Прикладное ПО |
| Cisco anyconnect | Специализиро­ванное ПО |
| КриптоПро CSP | СКЗИ |
| 6 | Server EFS DVB | Браузер Google Chrome | Специализированное ПО |
| Браузер Yandex | 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 |
| 7 | Server EFS DVB  Reserv | Браузер Google Chrome | Специализированное ПО |
| Браузер Yandex | 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 |

# СТРУКТУРА ОБРАБОТКИ ДАННЫХ И ТЕХНОЛОГИЧЕСКИЙ ПРОЦЕСС

ИС «ЕФС ДВБ» объединяет 5 АРМ пользователей:

* три АРМ дежурных специалистов;
* один АРМ лидера направления;
* один АРМ администратора ИС;

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

* физический сервер «Server EFS DVB Reserv», предназначенный для резервирования сервера ЕФС;
* физический сервер «Server EFS DVB», предназначенных для решения задач ЕФС;

Технологический процесс обработки информации в ИС «ЕФС 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 по эксплуатации 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 над 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 «ЕФС 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 «ЕФС 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 внутри объектового 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 «ЕФС ДВБ» предусмотрено резервное копирование данных, резервные копии файлов хранятся на физическом сервере ЕФС.

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

Антивирусная защита АРМ, входящих в состав ИС, обеспечивается средством антивирусной защиты «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 «ЕФС 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 удовлетворяет требованиям ГОСТ 51583. Этот документ является начальным для разработки технического проекта автоматизированной системы в защищенном исполнении.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. 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.
2. 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.
3. 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.
4. 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.
5. [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.
6. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.