Отчет об обследовании системы управления информационной безопасности

Региональный шлюз, как подсистема шлюза «электронного правительства» (Информационная система «Электронный акимат») Западно-Казахстанской области

Исполнитель

ОЮЛ «Центр анализа и расследования кибер атак»

_____ Рачев О.М.

«15» ноября 2019 г..

Принял

ГУ "Аппарат акима Западно-Казахстанской области"

_____

«4» 12 2019 г.

Уральск
2019 год

Аннотация

В настоящем документе приведены сведения об обследовании СУИБ ГУ "Аппарат акима Западно-Казахстанской области". Документ содержит общие сведения об организации, о состоянии ИТ-инфраструктуры и ИС, о целях развития ИТ и запланированных изменениях ИТ-инфраструктуры, об организационной структуре обеспечения ИБ, о процессах обеспечения ИБ и используемых средствах защиты информации организации, о законодательных, отраслевых и корпоративные требованиях в области обеспечения ИБ, об инструментальном контроле защищенности, выводы и рекомендации, перечень проведенных мероприятий по обследованию, план проведения интервью и соответствующие им протоколы.

Содержание

Перечень сокращений **5**

1 Общие сведения об организации **6**

2 Сведения об ИТ-инфраструктуре организации **7**

2.1 Системные требования 7

2.2 Физические сервера и АРМ 8

2.3 Мобильные устройства и съемные носители 8

3 Сведения об информационных системах организации **9**

3.1 Общие сведения 9

3.2 Структура 9

3.3 Компоненты 9

3.4 Логическая схема доступа пользователей 10

3.5 Сопровождение 10

3.6 Взаимодействие с сетью Интернет 10

3.7 Предоставление доступа 10

3.8 Контроль целостности и резервирование 11

4 Сведения об организационной инфраструктуре обеспечения ИБ организации **12**

5 Сведения о процессах обеспечения ИБ и используемых средствах защиты информации организации **13**

5.1 Внутренний контроль и аудит обеспечения ИБ 13

5.2 Управление доступом к информационным ресурсам 13

5.3 Управление уязвимостями информационных ресурсов 13

5.4 Управление изменениями в ИТ-инфраструктуре 13

5.5 Обеспечение непрерывности ИТ-сервисов 13

5.6 Сетевая безопасность 14

5.6.1 Защита сегментов доступа пользователей и серверов 14

5.7 Защита от утечек конфиденциальной информации 14

5.8 Резервное копирование 14

5.9 Обеспечение физической безопасности 14

5.10 Защита от вредоносного программного обеспечения 15

6 Сведения о законодательных, отраслевых и корпоративные требованиях в области обеспечения ИБ **16**

7 Сведения об инструментальном контроле защищенности 17

8 Проблемы, отмеченные представителями организации 18

9 Выводы и рекомендации 19

9.1 ИТ-инфраструктура организации 19

9.2 Организационная структура ИБ 19

9.3 Информационные системы 20

9.4 Процессы обеспечения ИБ 20

9.4.1 Внутренний контроль и аудит обеспечения ИБ 21

9.4.2 Управление доступом к информационным ресурсам 21

9.4.3 Управление уязвимостями информационных ресурсов 21

9.4.4 Управление изменениями в ИТ-инфраструктуре 22

9.4.5 Обеспечение непрерывности ИТ-сервисов 22

9.4.6 Обеспечение защиты конечных устройств 23

9.4.7 Сетевая безопасность 23

9.4.8 Защита от утечек конфиденциальной информации 23

9.4.9 Резервное копирование 24

9.4.10 Обеспечение физической безопасности 24

9.4.11 Защита от вредоносного программного обеспечения 24

9.4.12 Обеспечение целостности 25

9.4.13 Предоставление доступа контрагентам к защищаемой информации 25

9.5 Законодательные, отраслевые и корпоративные требованиях в области обеспечения ИБ 25

9.5.1 Законодательные требования 26

10 Перечень прилагаемых материалов 27

11 Сведения о результатах тестирования на проникновение 28

Перечень сокращений

АРМ	–	Автоматизированное рабочее место
ИБ	–	Информационная безопасность
ИС	–	Информационная система
Организация	–	ГУ "Аппарат акима Западно-Казахстанской области"
ЛВС	–	Локально-вычислительная сеть
РШЭП	–	Региональный шлюз, как подсистема шлюза «электронного правительства» (Информационная система «Электронный акимат») Западно-Казахстанской области
АО НИТ		АО «Национальные информационные технологии»
ПО	–	Программное обеспечение
ППО	–	Прикладное программное обеспечение
СКУД	–	Система контроля и управления доступом
Внешние пользователи	–	Государственные учреждения акимата Западно-Казахстанской области
Внутренние пользователи	–	Операторы; администратор; консультанты; разработчики

1 Общие сведения об организации

1.1 Полное наименование организации: ГУ "Аппарат акима Западно-Казахстанской области".

1.2 Юридический адрес: город Уральск, проспект Н.Назарбаева, 179.

1.3 ГУ "Аппарат акима Западно-Казахстанской области» осуществляет организационное, правовое, информационно-аналитическое, консультативное и материально-техническое обеспечение деятельности акимата и акима области.

1.4 Организация имеет в штате 60 работников.

2 Сведения об ИТ-инфраструктуре организации

2.1 Системные требования

Функциональная схема РШЭП состоит из трех уровней: уровень клиента, уровень сервера РШЭП, уровень резервного сервера БД (см. Рисунок 1).

Связь между клиентским уровнем и сервером РШЭП осуществляется через локальную сеть.

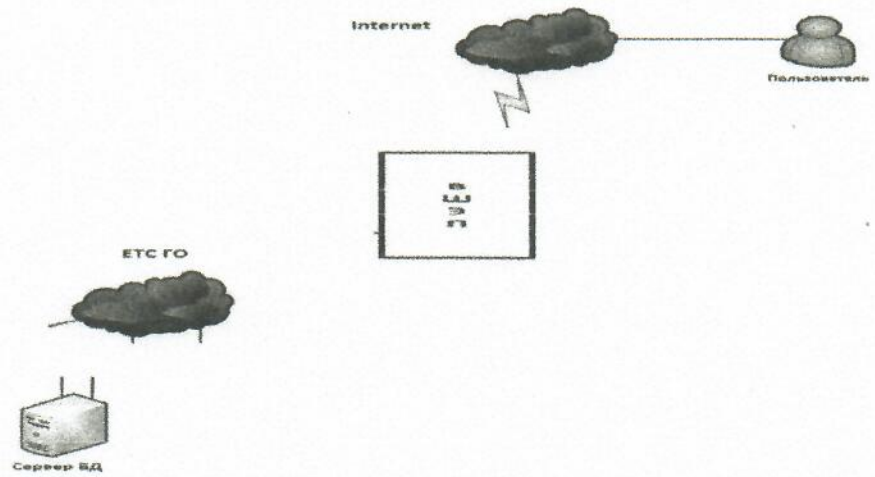

Рисунок 1 – Функциональная схема

Организация имеет использует серверную гермозону в АО «НИТ».

Доступ в серверную гермозону осуществляется в сопровождении администратора. Определен круг лиц, которые имеют право администрирования устройств.

Резервные копии проводятся на регулярной основе.

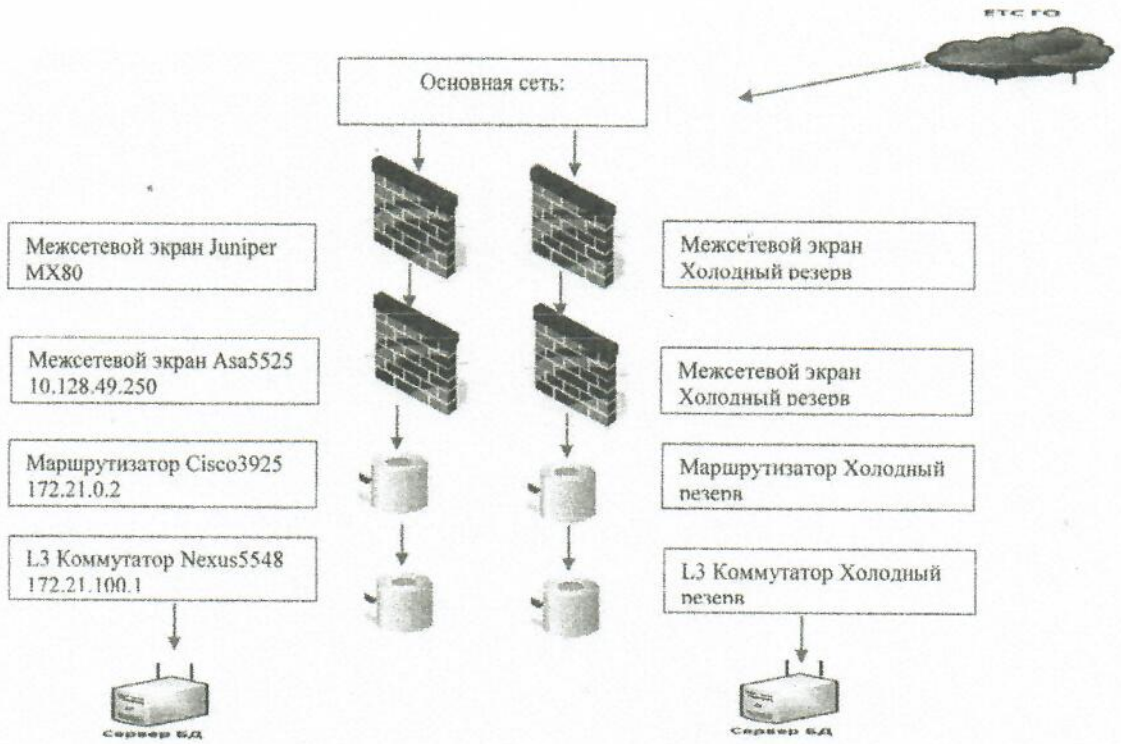

Рисунок 2- Схема сети передачи данных

2.2 Физические сервера и АРМ

Серверы РШЭП в количестве 2 единиц расположены на площадке в АО «НИТ».

В Организации эксплуатируется 393 единиц АРМ.

2.3 Мобильные устройства и съемные носители

Организация не использует корпоративные и личные смартфоны для осуществления доступа из сети Интернет в корпоративную среду.

USB-порты не заблокированы, Flash-диски не проверяются на наличие вирусов.

3 Сведения об информационных системах организации

3.1 Общие сведения

Официальный сайт Организации: **https://bko.gov.kz/**

3.2 Структура

РШЭП сопровождается специалистами АО «НИТ» и развернута на оборудованиях АО «НИТ».

3.3 Компоненты

№ п\п	Наименование сервера или виртуального ресурса (доменное имя, сетевое имя или логическое имя сервера)	Назначение (выполняемые функциональные задачи)	Кол-во	Характеристики сервера или используемых заявленных виртуальных ресурсов	ОС, СУБД, ПО, приложения, библиотеки и средства защиты, установленные на серверах или используемые виртуальные сервисы (состав программной среды с указанием номеров версий)	Применяемые IP -адреса
1	2	3	4	5	6	7
1	Eakimatserver3	Сервер №1	1	Intel ® Xeon® CPU, E7520@ 1,87 GHz 1,86 CHZ (2 процессора)	Windows Server 2008 R standart	10.236.1.239
2	Eakimatserver	Сервер №2 Резервный	1	ntel ® Xeon® CPU, E7520@ 1,87 GHz 1,86 CHZ (2 процессора)	Intel ® Xeon®	10.236.1.240

3.4 Логическая схема доступа пользователей

Работники ГУ "Аппарат акима Западно-Казахстанской области" являющиеся пользователями ИС, осуществляют доступ к ИС со своих АРМ.

Для ИС не предусмотрен удаленный доступ пользователей из сети Интернет с использованием веб-технологий (через портал).

Для регистрации в РШЭП внутренних и внешних пользователей в ИС необходимо пройти процедуры идентификации и аутентификации с использованием сертификата ЭЦП, однако для авторизации использование сертификата ЭЦП не требуется.

3.5 Сопровождение

Сопровождение прикладного программного обеспечения Поддержка аппаратного обеспечения РШЭП осуществляется специалистами АО «НИТ» по договору №24\17 -268 от 24.04.2019 года.

3.6 Взаимодействие с сетью Интернет

РШЭП не взаимодействует с сетью Интернет.

Пользователи имеют доступ к сети Интернет с других АРМ, не подключенных к сети РШЭП, для получения общедоступной информации, необходимой для выполнения должностных обязанностей. Доступ осуществляется по протоколам HTTP, HTTPS.

3.7 Предоставление доступа

Для доступа к РШЭП каждому пользователю присвоен уникальный идентификатор. Групповые учетные записи не используются.

При создании учетной записи средствами аутентификации систем устанавливается атрибут необходимости смены пароля при первом входе, во время первого входа пользователь самостоятельно формирует новый пароль с учетом требований парольной политики.

Доступ в РШЭП предоставляется с использованием паролей.

Личные пароли самостоятельно выбираются пользователями и администраторами ИС «Е-акимат» с учетом следующих требований:

1) длина пароля должна составлять не менее 8 символов;

2) в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и/или специальные символы (%,$,@, &, *, #, ^ и т.п.), в том числе вводимые через клавишу ALT;

3) запрещается при авторизации пользователя использовать только логин (имя пользователя) без пароля;

4) пароль не должен включать в себя легко вычисляемые сочетания символов (имена и даты рождения своей личности и своих родственников, номера автомобилей, телефонов и т.д.), которые можно угадать, основываясь на информации о пользователе, а также стандартное расположение букв на клавиатуре (zyxwvuts, 123, 123321, qwerty и т.д.);

5) рекомендуется использовать пароли случайного набора символов;

6) запрещается выбирать пароли, которые уже использовались ранее;

7) при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

8) пользователь не имеет права разглашать свои личный пароль.

3.8 Контроль целостности и резервирование

Для РШЭП осуществляется контроль целостности файлов и записей.

Для АРМ пользователей и серверов используется источник бесперебойного питания UPS.

4 Сведения об организационной инфраструктуре обеспечения ИБ организации

В организационно-штатной структуре Организации отсутствует специалист по ИБ. Функциональные обязанности по обеспечению ИБ в аппарате акима области и координации ИБ в структурных подразделениях возложены на главного инспектора отдела стратегического развития и цифровизации аппарата акима Западно-Казахстанской области, в соответствии с пунктом 30 должностной инструкции, утвержденной приложением к приказу руководителя аппарата акима Западно-Казахстанской области от 5.08.2019 года №196К.

Положение об отделе стратегического развития и цифровизации аппарата акима Западно-Казахстанской области, утвержденное приказом руководителя аппарата акима Западно-Казахстанской области от 2.08.2019 года №194К, согласно пунктам 4,8, 9 задачи 2 содержит следующие задачи в области ИБ

— контроль обеспечения политики ИБ в местных исполнительных органах;

— контроль исполнения требований технической документации по ИБ, контроль за управлением активами в части обеспечения ИБ, контроль за управлением рисками в сфере информационно-коммуникационных технологий, контроль за обеспечением непрерывности бизнес-процессов, использующих информационно-коммуникационных технологий;

— проведение внутреннего аудита ИБ, контроль за организацией внешнего аудита ИБ.

Необходимо определить конкретное лицо, перечень ответственности и полномочий за организацию системы информационной безопасности в Организации. В должностных инструкциях работников добавить обязанности по соблюдению требований ИБ, а также ответственность за их невыполнение.

5 Сведения о процессах обеспечения ИБ и используемых средствах защиты информации организации

5.1 Внутренний контроль и аудит обеспечения ИБ

Регулярный контроль и аудит обеспечения ИБ в Организации не проводился.

5.2 Управление доступом к информационным ресурсам

Предоставление доступа работнику осуществляется на основании заявки. В заявке указывается перечень систем и ресурсов, к которым необходим доступ, а также требуемые полномочия доступа.

Доступ может быть заблокирован в случае:

- увольнения;
- перевод на другую должность;
- долгосрочный отпуск (более 1 месяца).

Блокировку доступа осуществляют работники АО «НИТ».

Владельцем процесса управления доступом к информационным ресурсам является АО «НИТ».

5.3 Управление уязвимостями информационных ресурсов

Аудиты на проверку уязвимостей в Организации не проводились.

5.4 Управление изменениями в ИТ-инфраструктуре

Необходимо разработать и утвердить документ «Руководства администратора» с указанием ответственности за внесение изменении в ИТ-инфраструктуру.

5.5 Обеспечение непрерывности ИТ-сервисов

Не обеспечивается резервирование всех компонентов, которые обеспечивают функционирование ИТ-инфраструктуры.

План обеспечения непрерывности при наступлении каждого идентифицированного события не разработан.

5.6 Сетевая безопасность

5.6.1 Защита сегментов доступа пользователей и серверов

Пользовательские АРМ подключены в сегментах, отделенных от серверного сегмента. Происходит фильтрация трафика между пользовательскими сегментами и серверными сегментом.

Серверы различных систем располагаются в соответствующих сегментах в зависимости от функциональных характеристик ИС, сервер расположен в зоне ДМЗ.

Сегменты пользователей разделены по принадлежности к структурным подразделениям Организации – сегмент для сотрудников, отдельный для руководства Организации, отдельный сегмент для подрядчиков.

Сетевой доступ между рабочими станциями пользователей заблокирован. Доступ может быть предоставлен администратором по согласованной заявке.

5.7 Защита от утечек конфиденциальной информации

Контроль утечек конфиденциальной информации не проводится.

5.8 Резервное копирование

Резервное копирование осуществляется на регулярной основе сотрудниками АО «НИТ».

Для описания полного процесса резервного копирования необходимо разработать документ «Правила резервного копирования информации и программного обеспечения Организации».

5.9 Обеспечение физической безопасности

Доступ в серверные помещения РШЭП контролируется сотрудниками АО «НИТ». Посещение серверных помещений разрешено ограниченному числу лиц, в присутствии ответственного лица за серверное помещение.

На шкафах с серверным и сетевым оборудованием имеются двери и замки.

Видеокамера установлена внутри гермозоны.

Посетители в здание АО «НИТ» проходят через охрану, с отметкой в журнале.

5.10 Защита от вредоносного программного обеспечения

Для защиты рабочих станций от вредоносного ПО установлен антивирус ESET. На серверах установлен антивирус ESET Endpoint Antivirus 5.0.2126.3.

6 Сведения о законодательных, отраслевых и корпоративные требованиях в области обеспечения ИБ

В Организации определен порядок по защите служебной информации, в соответствии с Этическим кодексом государственных служащих Республики Казахстан (Правила служебной этики государственных служащих), утвержденным Указом Президента Республики Казахстан от 29 декабря 2015 года № 153.

Требования законодательства к ЭЦП не применимы, т.к. Организация не осуществляется их выпуск. В Организации используются ЭЦП созданные и предоставленные Национальным удостоверяющим центром для участия в государственных закупках и взаимодействия с государственными органами.

Ответственность за сохранность ЭЦП возложена на работников. ЭЦП хранятся на токенах и flash-носителях. Кроме того, осуществляется учет ЭЦП, выданных и отозванных Национальным удостоверяющим центром.

Национальные стандарты Республики Казахстан в области защиты информации используются в Организации в качестве методических пособий.

Отраслевые требования отсутствуют.

Проверки соответствия законодательным требованиям и требованиям внутренних нормативных документов в области обеспечения ИБ не проводились.

7 Сведения об инструментальном контроле защищенности

Внешнее и внутреннее сканирование было произведено с использованием следующего ПО: Metasploit Framework, OWASP Zap, nmap, а также вспомогательные модули к данному ПО, в том числе, собственной разработки. Анализ наличия ложно-позитивных и ложно-негативных результатов автоматической проверки проводится вручную, также как и оценка полученных в результате сканирования данных и последующая эксплуатация. Полученные при сканировании результаты и способы их успешной эксплуатации будут приведены в отчете по тестированию на проникновение.

8 Проблемы, отмеченные представителями организации

Проблемы, отмеченные представителями организации в рамках проведенного обследования, не выявлены.

9 Выводы и рекомендации

9.1 ИТ-инфраструктура организации

Автоматизация существующих бизнес-процессов Организации осуществляется с использованием ИТ-инфраструктуры, состоящей из следующих ключевых элементов: ЛВС, каналы связи, АРМ и сервера.

В отношении ИТ-инфраструктуры рекомендуется выполнить следующие мероприятия, направленные на повышение эффективности обеспечения ИБ Организации:

1) Предусмотреть для каждого устанавливаемого обновления процедуру отката, а также разработать и утвердить для этого соответствующие инструкции.
2) Документировать перечень ПО, необходимого для функционирования серверов ИС, а также АРМ пользователей и администраторов (отсутствие перечня ПО, необходимого для функционирования серверов информационных ресурсов и АРМ, не позволяет эффективно контролировать активные сервисы на устройствах. Наличие избыточных активных сервисов повышает риск компрометации информационных ресурсов).
3) Внедрить ПО для контроля целостности и настроить его на контроль целостности конфигурационных файлов или директорий, в которых они располагаются для ОС, СУБД, сетевых устройств и ППО ИС.
4) Осуществлять шифрование резервных копий информации для их безопасного хранения. Рассмотреть возможности используемого в Организации ПО для создания резервных копий в части встроенного функционала по шифрованию резервных копий.

9.2 Организационная структура ИБ

В Организации определено структурное подразделение, ответственное за обеспечения безопасности - Отдел стратегического развития и цифровизации аппарата акима Западно-Казахстанской области.

Необходимо определить конкретное лицо, перечень ответственности и полномочий за организацию системы информационной безопасности в Организации.

9.3 Информационные системы

По всем ИС Организации необходимо выполнить мероприятия, направленные на повышение эффективности обеспечения их ИБ (с учетом процесса обработки информации в ИС и встроенных механизмов защиты).

9.4 Процессы обеспечения ИБ

Текущий уровень зрелости процессов ИБ Организации представлен на рисунке 3

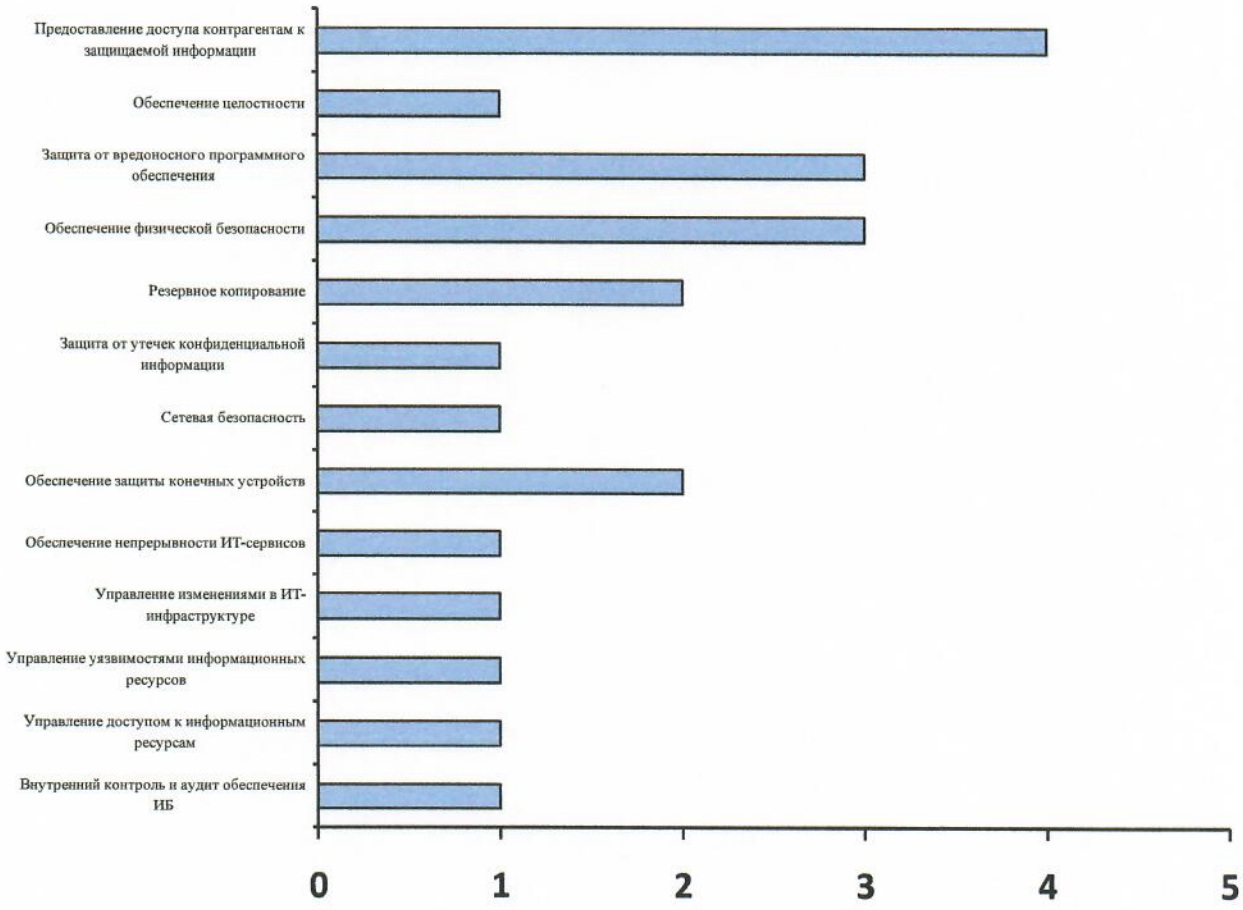

Рисунок 3 –Текущий уровень зрелости процессов обеспечения ИБ

Рекомендации в отношении каждого обследованного процесса обеспечения ИБ приведены ниже.

9.4.1 Внутренний контроль и аудит обеспечения ИБ

Уровень зрелости процесса определен как **первый.**

Для повышения уровня зрелости процесса рекомендуется выполнить следующие мероприятия:

1) Необходимо разработать регламентирующий нормативный документ касательно процедуры проведения внутреннего аудита ИБ;
2) Пройти обучение по курсу внутренний аудитор ИБ.

9.4.2 Управление доступом к информационным ресурсам

Уровень зрелости процесса определен как **первый**.

Для повышения уровня зрелости процесса рекомендуется выполнить следующие мероприятия:

3) Необходимо разработать регламентирующий нормативный документ касательно процедуры предоставления доступов, утвердить перечень владельцев ИС;
4) Рекомендуется разработать и утвердить матрицу ролей и учётных записей комплекса, в которой будут определены права и роли для каждого пользователя и группы пользователей;
5) Рекомендуется разработать регламентирующий документ касательно регистрации пользователей и администраторов ИС в корпоративной сети;
6) Разработать регламентирующую процедуру, включая требования по удалению и блокированию уволенных работников

9.4.3 Управление уязвимостями информационных ресурсов

Уровень зрелости процесса определен как **первый**.

Для повышения уровня зрелости процесса рекомендуется выполнить следующие мероприятия:

1) Документировать процесс управления уязвимостями, в котором предусмотреть мероприятия, направленные на документирование и согласование запланированных действий по устранению выявленных уязвимостей.

2) Для повышения эффективности выявления уязвимостей используемого ПО и сетевых протоколов использовать автоматизированные сканеры безопасности.

3) Осуществлять контроль его выполнения (например, в рамках проведения внутренних аудитов ИБ).

9.4.4 Управление изменениями в ИТ-инфраструктуре

Уровень зрелости процесса определен как **первый**.

Для повышения уровня зрелости процесса рекомендуется выполнить следующие мероприятия:

1) Документировать процесс управлениями изменениями в ИТ-инфраструктуре, в котором предусмотреть мероприятия, направленные на документирование и согласование запланированных действий по внесению изменений в ИТ-инфраструктуру Организации, а также мероприятия по тестированию внедряемые изменений.

2) Осуществлять контроль его выполнения (например, в рамках проведения внутренних аудитов ИБ).

9.4.5 Обеспечение непрерывности ИТ-сервисов

Уровень зрелости процесса определен как **первый**.

Для повышения уровня зрелости процесса рекомендуется выполнить следующие мероприятия:

1) Для критичных компонентов ИТ-инфраструктуры определить и задокументировать максимальное время простоя.

2) Идентифицировать и задокументировать все события, из-за которых возможны остановки компонентов ИТ-инфраструктуры (и как следствие, полная либо частичная остановка бизнес-процессов).

3) Для идентифицированных событий, из-за которых возможны остановки компонентов ИТ-инфраструктуры:

- определить вероятность их наступления;
- определить ущерб от их наступления;
- разработать планы обеспечения непрерывности при наступлении каждого идентифицированного события.

4) Документировать процесс обеспечения непрерывности ИТ-сервисов.

5) Осуществлять контроль его выполнения (например, в рамках проведения внутренних аудитов ИБ).

9.4.6 Обеспечение защиты конечных устройств

Уровень зрелости процесса определен как **второй**.

Для повышения уровня зрелости процесса рекомендуется выполнить следующее:

1) Предоставить пользователям средства для шифрования защищаемой информации, обрабатываемой на съемных носителях.

9.4.7 Сетевая безопасность

Уровень зрелости процесса определен как **первый**.

Для повышения уровня зрелости процесса рекомендуется выполнить следующие мероприятия:

1) Разработать и утвердить документ, регламентирующий разделение корпоративной сети, порядок внесения правил в сетевые устройства,
2) разработать логическую топологию сети.

9.4.8 Защита от утечек конфиденциальной информации

Уровень зрелости процесса определен как **первый**.

Для повышения уровня зрелости процесса рекомендуется выполнить следующие мероприятия:

1) Для повышения эффективности обнаружения и предотвращения утечек рассмотреть возможность внедрения специализированного средства защиты информации класса DLP.

2) Осуществлять контроль его выполнения (например, в рамках проведения внутренних аудитов ИБ).

9.4.9 Резервное копирование

Уровень зрелости процесса определен как **второй**.

Для повышения уровня зрелости процесса рекомендуется выполнить следующие мероприятия:

1) Документировать процесс резервного копирования в отношении компонентов ИТ-инфраструктуры (включая ИС).

3) Документировать места хранения резервных копий.

4) Осуществлять контроль целостности файлов резервных копий.

5) Проводить тестирование работоспособности резервных копий.

6) Осуществлять контроль его выполнения (например, в рамках проведения внутренних аудитов ИБ).

9.4.10 Обеспечение физической безопасности

Уровень зрелости процесса определен как **третий**.

Для повышения уровня зрелости процесса рекомендуется выполнить следующие мероприятия:

1) Рассмотреть целесообразность установки СКУД на серверное помещение.

2) Осуществлять контроль его выполнения (например, в рамках проведения внутренних аудитов ИБ).

9.4.11 Защита от вредоносного программного обеспечения

Уровень зрелости процесса определен как **третий**.

Для повышения уровня зрелости процесса рекомендуется выполнить следующие мероприятия:

1) Документировать порядок обеспечения антивирусной защиты информационных ресурсов Организации.

2) Разработать инструкцию для пользователей, в которой сформулировать правила по обеспечению антивирусной защиты при работе с информационными технологиями.

3) Внедрить специальные антивирусные средства для защиты рабочих станций и виртуальной среды.

4) Осуществлять контроль его выполнения (например, в рамках проведения внутренних аудитов ИБ).

9.4.12 Обеспечение целостности

Уровень зрелости процесса определен как **первый**.

Для повышения уровня зрелости процесса рекомендуется выполнить следующие мероприятия:

1) Разработать и документировать порядок обеспечения целостности компонентов ИТ-инфраструктуры.

2) Внедрить ПО для контроля целостности и настроить контроль целостности конфигурационных файлов (или директорий, в которых они располагаются) ОС, СУБД, сетевых устройств и ППО ИС, а также резервных копий информационных ресурсов.

3) Осуществлять контроль его выполнения (например, в рамках проведения внутренних аудитов ИБ).

9.4.13 Предоставление доступа контрагентам к защищаемой информации

Уровень зрелости процесса определен как **четвертый**.

Для повышения уровня зрелости процесса рекомендуется выполнить следующие мероприятия:

1) Документировать порядок предоставления доступа контрагентам к защищаемой информации.

2) Осуществлять контроль его выполнения (например, в рамках проведения внутренних аудитов ИБ).

9.5 Законодательные, отраслевые и корпоративные требованиях в области обеспечения ИБ

9.5.1 Законодательные требования

В Организации не в полной мере выполняются требования нормативно-правовых актов Республики Казахстан в области защиты информации.

Для соответствия им рекомендуется выполнить следующие мероприятия:

1) Осуществить разработку моделей угроз (проведение оценки рисков) в отношении обрабатываемых персональных данных и осуществлять их периодическую актуализацию, в том числе, в случае изменения порядка обработки персональных данных, изменения технических и программных средств обработки персональных данных, изменения технологии обработки персональных данных.
2) Периодическую актуализацию перечня ИКТ.
3) Осуществлять периодическую актуализацию перечня лиц, имеющих право свободного доступа к ИКТ.

Национальные стандарты Республики Казахстан носят рекомендательный характер и могут быть использованы Организациям по своему усмотрению.

10 Перечень прилагаемых материалов

Перечень прилагаемых материалов представлен ниже.

№	Название документа
1	Политика информационной безопасности
2	Правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации
3	Методика оценки рисков ИБ
4	Правила инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения
5	Правила проведения внутреннего аудита ИБ
6	Правила использования сети Интернет и электронной почты
7	Правила использования средств криптографической защиты информации
8	Правила организации процедуры аутентификации
9	Правила разграничения прав доступа к электронным информационным ресурсам
10	Правила организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов
11	Правила использования мобильных устройств и носителей информации
12	Правила организации антивирусного контроля
13	Руководство администратора по сопровождению объекта информатизации
14	Регламент резервного копирования и восстановления информации
15	Инструкция о порядке действий пользователей по реагированию на инциденты информационной безопасности и во внештатных (кризисных) ситуации
16	Правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации