Утверждено:
Решением Совета директоров
АО «Сентрас Секьюритиз»
Протокол № 75 от 21.04.2010 года
Внесены изменения:
Решением СД от 28.06.2012 г.
Решением СД от 10.06.2014 г. (новая редакция)
Решением СД от 30.04.2021 г. (новая редакция)
Решением СД от 15.04.2022 г. (новая редакция)
Решением СД от 30.09.2022 г. (новая редакция)
Решением СД от 30.01.2023 г. (новая редакция)
Решением СД от 06.10.2023г. (новая редакция)
Решением СД от 29.01.2024г. (новая редакция)
Решением СД от 30.10.2024г. (новая редакция)

Правила обеспечения информационной

безопасности АО «Сентрас Секьюритиз»

Алматы, 2024 год

Оглавление

Настоящие Правила разработаны согласно требованиям законодательства Республики Казахстан и определяют минимально необходимый функционал информационных систем АО «Сентрас Секьюритиз» (далее - Компания), набор требований к обеспечению информационной безопасности при обработке информации, содержащей коммерческую тайну, а также содержат описание политики информационной безопасности.

Все, что не предусмотрено по информационным системам в настоящих Правилах, помимо норм законодательства, Компания руководствуется нормами Инструкции к программному обеспечению ведения бухгалтерского учета.

Настоящие Правила анализируются и пересматриваются при возникновении существенных изменений в законодательстве либо в процессах Компании.

Перечень лиц и порядок их взаимодействия с компетентными органами: первый руководитель Компании или лицо, его замещающее взаимодействует от имени Компании с компетентными органами (правоохранительные органы, пожарные службы, уполномоченный орган по контролю и надзору за деятельностью финансовых организаций и другие государственные органы) и самостоятельно принимает необходимые решения, а также ведет переписку или переговоры, подписывает документы.

Компания поддерживает взаимодействие своих работников по информационной безопасности с профессиональными группами, ассоциациями и направляет своих работников для участия в конференциях (форумах), на обучения по информационной безопасности.

Используемые в Правилах понятия и термины

1) информационные системы (далее - ИС) - организационно упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач;

2) пользователь (работник) - сотрудник Компании, которому предоставляется необходимый доступ в информационные системы Компании, а также необходимое оборудование, закрепленное за ним при зачислении на штатную должность, для исполнения должностных обязанностей;

3) ответственное подразделение - подразделение Компании, за которым закреплено выполнение определенных функций, согласно положению о подразделении Компании или настоящими Правилами (ДИТ или СИБ, соответственно);

ДИТ – Департамент информационных технологий;

СИБ – Служба информационной безопасности;

4) специалист ответственного подразделения (ДИТ или СИБ, соответственно)- пользователь подразделения Компании, за которым закреплено выполнение определенных функций, согласно должностной инструкции Компании или настоящими Правилами;

5) технологическая учетная запись - учетная запись пользователя в информационной системе, предназначенная для аутентификации при взаимодействии с информационными системами;

6) привилегированная учетная запись (администратор ИС) - учетная запись в информационной системе, обладающая привилегиями создания, редактирования, блокирования и удаления технологических учетных записей пользователя, в том числе обладающая привилегиями изменения прав доступа технологических учетных записей пользователя, а также наделенная правами конфигурирования информационной системы или группы информационных систем, закрепленная за пользователем;

7) заявка - обращение пользователя, при необходимости утвержденное непосредственным руководителем, предоставленное в бумажном или электронном виде в ответственное подразделение для осуществления организационно-технических мероприятий, связанных с установкой программного обеспечения и предоставлением доступа к информационным системам и помещениям Компании, а также установкой, приобретением, подключением и отключением периферийного и иного оборудования;

8) предоставление доступа к информационным системам Компании (доступ) - комплекс организационно-технических мероприятий по созданию и редактированию технологических

учетных записей, а также уровня прав доступа в информационные системы Компании, в объеме, необходимом для исполнения пользователем должностных обязанностей;

9) ограничение доступа к информационным системам Компании (блокирование/аннулирование) - комплекс организационно-технических мероприятий по блокированию и/или отключению технологических учетных записей пользователя, а также изменению и/или аннулированию прав доступа пользователя в информационные системы Компании;

10) оборудование пользователя - рабочая станция, ноутбук, мобильное устройство и иное оборудование, закрепленное за пользователем, по средствам которого ему предоставляется необходимый доступ в информационные системы Компании, для исполнения должностных обязанностей;

11) рабочая станция - стационарный персональный компьютер пользователя информационной системы Компании, с установленным программным обеспечением и периферийным оборудованием;

12) ноутбук - персональный компьютер, исполненный в форме, удобной для переноски и использования в том числе, за пределами периметра защиты;

13) мобильное устройство - электронное устройство индивидуального пользования, функционирующее на основе мобильной версии операционной системы;

14) серверы - компьютерное оборудование Компании, предназначенное для работы информационных систем Компании, а также для предоставления доступа к информационным системам Компании с авторизацией пользователей и контролем уровня прав доступа в информационных системах;

15) администратор сервера - специалист ДИТ, отвечающий за работоспособность, безопасность, целостность данных и информационных систем сервера;

16) паспорт сервера - документ, содержащий в себе полную информацию, предусмотренную настоящими Правилами;

17) периферийное оборудование - устройства, являющиеся частью или совместимые с компьютером (кроме системного блока, клавиатуры, мыши, сетевого адаптера и монитора): принтеры, сканнеры, модемы, внешние носители информации и др.;

18) носитель информации - внутренние устройства для долговременного хранения информации (например, CMOS-память, жёсткие диски, SSD), которые записывают, хранят и воспроизводят данные, которые обрабатываются благодаря вычислительной технике.

19) пломбирование оборудования - опечатывание оборудования пользователя или сервера путем наклеивания в места блокировки корпуса специальной пломбы (бумажной ленты), с целью исключения несанкционированных аппаратных изменений;

20) локальная вычислительная сеть Компании (далее - локальная сеть) - система распределенной обработки данных, охватывающая небольшую территорию, состоящая из структурированной кабельной сети, активного и пассивного сетевого оборудования, периферийного оборудования, серверов и рабочих станций, обеспечивающая функционирование структурных подразделений Компании, доступ к информационным системам, совместное использование ресурсов, обмен и передачу информации, а также доступ к Интернет ресурсам;

21) активное сетевое оборудование - коммуникационные средства (коммутаторы, маршрутизаторы, мосты и т.п.), предназначенные для объединения серверов и компьютеров пользователей в локальную сеть;

22) информационная безопасность - практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации;

23) обеспечение информационной безопасности - процесс, направленный на поддержание состояния конфиденциальности, целостности и доступности информации и информационных систем Компании;

24) журнал сервера - специализированное средство, разработанное с целью отражения штатных и критических действий в процессе функционирования информационных систем;

25) резервная копия - актуальная копия данных на носителе информации, предназначенная для восстановления данных в оригинальном или новом месте их расположения в случае повреждения или разрушения информационных систем, а также эталонные исходные коды, при наличии;

26) защищаемая информация - конфиденциальная информация, содержащая инсайдерскую и коммерческую тайну на рынке ценных бумаг, предусмотренную настоящими Правилами и законодательством РК.

Раздел 1. Пользователи

1.1 Порядок действий пользователей при приеме на работу

1. Пользователь при подписании трудового договора: получает оборудование пользователя, необходимое периферийное оборудование, электронный ключ/карту доступа в офисное помещение, закрепляемое за ним при зачислении на штатную должность, а также необходимый доступ в ИС, согласно должностным инструкциям.

Все работники Компании (в том числе руководство Компании) в обязательном порядке знакомятся с настоящими Правилами, после чего обязуются соблюдать требования настоящих Правил и прикладывать все возможные усилия по обеспечению информационной безопасности.

1.2 Порядок действий пользователей при переводе и расторжении (прекращении) трудового договора

1. Перенос предоставленного пользователю Компанией оборудование пользователя и периферийных устройств на другое место, даже в пределах офисного помещения, в обязательном порядке согласовывается с ДИТ.
2. При переводе или перемещении пользователя из одного структурного подразделения в другое, а также при расторжении (прекращении) трудового договора с работником, пользователь обязан предоставить возможность руководителю структурного подразделения скопировать служебную информацию с оборудование пользователя на сетевой ресурс или на оборудование пользователя руководителя структурного подразделения. Контроль за переносом конфиденциальной информации с оборудование пользователя возлагается на руководителя структурного подразделения. Ненужная информация удаляется руководителем структурного подразделения. Затем пользователь сдает оборудование пользователя, периферийное оборудование, электронный ключ доступа в офисное помещение и все сопутствующее оборудование специалистам ДИТ, после чего специалисты ДИТ производят замену пароля или блокировку/аннулирование учетных записей в ИС.
3. При переводе пользователя в другое подразделение пересматривается уровень доступа в ИС, согласно новой должностной инструкции пользователя.

1.3 Обязанности и ограничения пользователя при работе

1. Пользователь обязан ежемесячно изменять персональный пароль учетной записи согласно требованиям к паролю используемый для входа в ИС. Все требования к паролю изложены в пункте 4.3 Раздела 4 настоящих Правил.
2. Пользователь обязан отходя от рабочего места производить блокировку использованного оборудования и ИС для исключения возможности получения доступа к оборудованию и ИС третьими лицами.
3. Пользователю категорически запрещается:

– вход в ИС и/или доступ к сетевым ресурсам без прохождения авторизации пользователя;

– изменение системных каталогов и их содержимого на оборудовании пользователя (WINDOWS, Program Files и другие), а также любое изменение структуры каталогов на сетевых дисках/ресурсах;

– хранить на локальных или сетевых дисках/ресурсах информацию, не относящуюся к его непосредственной работе (файлы видео, файлы аудио, графические файлы и т.п.). Данная информация, при ее обнаружении, будет удалена без предупреждения;

– предоставлять доступ по локальной сети к своим локальным файлам, каталогам, жестким дискам и т.п., размещенным на закрепленном за ним оборудовании;

– передавать сетевое имя своего оборудования и IP адрес, свою учетную запись (логин/пароль) от ИС третьим лицам, а также хранить данные для авторизации в ИС в открытом доступе;

– производить любые изменения в подключениях сетевого кабеля (LAN) к оборудованию пользователя и на сетевом оборудовании;

– производить самостоятельное подключение личного оборудования к локальной сети Компании;

– самостоятельно пытаться устанавливать любое ИС на свое оборудование пользователя.

1.4 Ответственность пользователей при работе

1. Пользователь несет личную ответственность за:

– сохранность и целостность предоставленного ему Компанией оборудования и периферийных устройств;

– за целевое использование периферийного оборудования;

– сохранность информации, находящейся на оборудование пользователя;

– содержание передаваемой по локальной сети Компании информации;

– содержание информации, пересылаемой по электронной почте.

2. Все пользователи обязаны обеспечивать информационную безопасность и неукоснительно соблюдать требования настоящих Правил, а также незамедлительно уведомлять СИБ о нарушениях информационной безопасности. Пользователи периодически, не менее одного раза в год (в устном порядке или путем уведомления по электронной почте) оповещаются о необходимости уведомлять СИБ о нарушениях информационной безопасности.

3. В случае нарушения или несоблюдения настоящих Правил и/или процедур по информационной безопасности, повлекшие за собой:

– массовое заражение известными вирусами информационным системам Компании;

– утрату или хищение конфиденциальной и финансовой информации;

– увеличение трафика во внешней или внутренней сети (например, не имеющие отношение к работе почтовые рассылки анекдотов, изображений, музыки, фильмов);

– создание предпосылок к несанкционированному доступу к информационным системам Компании в том числе третьими лицами, пользователи могут быть привлечены к дисциплинарной ответственности и/или дисциплинарному взысканию в рамках Трудового Кодекса Республики Казахстан, в соответствии с выводами по материалам служебного расследования, вплоть до расторжения трудового договора, или передачи материалов в правоохранительные органы. Технологическая учетная запись пользователя может быть заблокирована до принятия решения по инциденту.

4. При обнаружении нестандартной/форс-мажорной ситуации с данными на своем оборудовании пользователя или в ИС пользователь обязан незамедлительно информировать своего руководителя и специалистов ДИТ о выявленной ситуации. До их прибытия пользователю запрещается производить какие-либо действия на своем оборудовании пользователя, например, изменять информацию в ИС, удалять или изменять любые файлы, закрывать ИС, выключать или перезагружать оборудование пользователя.

5. Контроль за соблюдением требований настоящих Правил пользователями осуществляется ответственным подразделением СИБ или ДИТ, соответственно их функциям. Контроль за соблюдением информационной безопасности, регистрация инцидентов осуществляется СИБ в соответствующем журнале.

1.5 Правила использования и ограничения в электронной переписке для пользователя (включая электронную почту)

1. Запрещается передавать свою учетную запись (логин/пароль) от корпоративной электронной почты, а также предоставлять доступ в корпоративную электронную почту пользователя третьим лицам.

2. Использование внешних почтовых электронных адресов разрешено в случае острой служебной необходимости и допускается только в случае принятия электронной почты на личный электронный ящик - через ДИТ.

3. Запрещается посредством почтовых серверов Компании рассылать развлекательные видео, аудио -файлы. Исключением могут быть только нужные для служебной необходимости файлы.

4. Запрещается заниматься массовой рассылкой сообщений людям, не давшим согласие на их получение.

5. При получении пользователем по электронной почте писем/сообщений из неизвестных источников с сомнительным содержанием/ссылками/вложением, пользователь обязан до открытия вложений и/или перехода по ссылке оповестить СИБ.

6. При оформлении электронного письма пользователь обязан поставить свою корпоративную подпись и указать тему письма. Сообщения, отправленные без указания темы, до получателя не дойдут и будут автоматически удалены. В этом случае ответственность за срыв проекта, сроков сдачи или предоставления информации, лежит на самом отправителе сообщения без указания темы.

7. Документы и файлы защищаемой информации, передаваемые посредством почтовых серверов, в обязательном порядке должны быть согласованы и одобрены к передаче непосредственным руководителем. Если это конфиденциальная информация, рекомендуется запаковать в архив с паролем или добавить пароль на открытие файла/файлов средствами офисного приложения. Пароль к архиву можно передать по телефону, SMS-кой, через Skype, любым другим способом, кроме как в самом электронном сообщении с файлом.

1.6 Правила использования и ограничения в использовании Интернет-ресурсов для пользователя

1. Запрещается загрузка аудио и видео файлов из Интернет-ресурсов. В случае служебной необходимости скачать аудио и видео материалы можно обратившись в ДИТ.

2. Запрещается самостоятельная загрузка пользователем исполнительных программ и скриптов.

3. Пользователям при работе с Интернет-ресурсами рекомендуется:

– использовать надежные пароли;

– по возможности включать многофакторную аутентификацию учетной записи;

– убедиться, что веб-сайты выглядят и работают надежно, соответствие адреса веб-сайта и использование сертификата безопасности (в ином случае не рекомендуется вносить на таком веб-сайте личные/ платежные данные и пароли);

– оценить и ознакомиться с параметрами и политиками конфиденциальности;

– следить, по каким ссылкам вы переходите;

– быть осторожными с загружаемыми из интернета файлами (при загрузке файлов проводить их проверку на вирусы до открытия);

– быть осторожными с информацией, публикуемой в интернете, поскольку при удалении оригинала не происходит удаление копий, которые могли сделать другие пользователи;

– перепроверять найденную в интернете информацию.

1.7 Правила использования и ограничения в работе с файлами и информацией

1. Файлы, расположенные на «Рабочем столе», хранятся только на оборудовании пользователя, без сохранения резервной копии при этом, не рекомендуется пользователю сохранять рабочие документы на «Рабочем столе». Пользователю рекомендуется сохранение рабочих документов и другой важной информации на сервере, в рабочей папке своего подразделения (у каждого подразделения на сервере имеется своя рабочая папка).

2. Для обмена и быстрой передачи разрешенными файлами и информацией между подразделениями имеется специальная общая папка с полным доступом для всех авторизованных пользователей. Данная папка очищается 1 раз в месяц, без предупреждения пользователей.

3. Пользователям запрещается свободное копирование файлов и информации на внешние носители информации. В случае производственной необходимости допускается копирование файлов и информации на внешние носители информации, в целях дальнейшего перемещения информации за пределы офисного помещения. Для выполнения данного мероприятия пользователем подается служебная записка руководителю Компании и после ее одобрения осуществляется копирование заявленной информации ДИТ. Каждая попытка использования внешнего носителя информации на оборудовании пользователя фиксируется и предоставляется по запросу непосредственного руководителя.

4. По факту обнаружения попытки несанкционированного копирования информации и/или выноса за пределы офисного помещения внешних носителей информации пользователем - инициируется служебное расследование.

Раздел 2. Порядок доступа в офисное помещение и помещения специального назначения

2.1 Доступ в офисное помещение

1. Свободный доступ в офисное помещения ограничен. Доступ в офисное помещение возможен только при наличии электронного ключа/карты с соответствующим уровнем доступа.
2. Для выпуска электронного ключа/карты для пользователя специалистом HR передается необходимая информация по пользователю в ДИТ.
3. Доступ в офисное помещение третьих лиц разрешен только в присутствии специалиста ДИТ.

2.2 Доступ в помещения специального назначения (серверное помещение/ЦОД)

1. В серверном помещении расположены серверное и телекоммуникационное оборудование, системы бесперебойного питания. Серверное помещение располагается в отдельном помещении, оснащенное системой пожарной безопасности, видеонаблюдением и рекомендованной производителем системой поддержания микроклимата с оповещением ответственных лиц (оборудовано системой охлаждения воздуха для поддержания благоприятной температуры и влажности воздуха в помещении).
2. Серверное помещение является помещением ограниченного доступа. Постоянный доступ к нему имеют только специалисты ДИТ.
3. Доступ посторонних людей в серверное помещение возможен только в присутствии специалиста ДИТ. В этом случае, ответственность за любые нарушения доступа возлагается на специалиста ДИТ.
4. Доступ в серверное помещение возможен только при наличии физического и электронного ключа/карты. Ответственным лицом за физический и электронный ключ/карту от серверного помещения является специалист ДИТ.
5. Дверь в серверное помещение постоянно должна быть запертой. Вход в серверное помещение фиксируется системой контроля доступа. В серверном помещении ведется постоянное видеонаблюдение.

Раздел 3. Информационные системы (ИС)

3.1 Порядок установки ИС, устанавливаемых на оборудование пользователей

1. Руководитель структурного подразделения формирует заявку на установку ИС, необходимой для выполнения должностных обязанностей, персонально для каждого пользователя. Руководители структурных подразделений несут ответственность за соответствие должностных обязанностей пользователей заявляемым программным продуктам, периферийному оборудованию и доступу к сетевым ресурсам и ИС.
2. Если необходимые ИС приобретены, и имеются клиентские лицензии, специалисты ДИТ устанавливают ИС, указанное в заявке.
3. На оборудование пользователей разрешается установка только лицензионного, условно-бесплатного, бесплатного, свободно распространяемого с открытым кодом (GNU), официально

поддерживаемого в части обновлений безопасности. Использование пиратских копий ИС, а также ИС для домашнего использования категорически запрещается.

4. Для защиты ИС используется лицензионное антивирусное программное обеспечение или системы, обеспечивающие целостность и неизменность программной среды на оборудовании пользователей. Используемое антивирусное программное обеспечение соответствует требованиям законодательства РК. На всех оборудованиях пользователей и серверах проводится своевременное обновление антивирусных баз для антивирусного программного обеспечения.

5. Специалистами ДИТ обеспечивается своевременная установка обновлений безопасности ИС. Обновления безопасности ИС, устраняющие критичные уязвимости, устанавливаются не позднее двух месяцев со дня их публикации и/или распространения производителем.

6. Проводится в автоматическом режиме на периодической основе (ежедневно) сканирование на наличие вредоносного программного кода и на предмет выявления критических уязвимостей в ИС с оповещением специалиста СИБ.

7. При выявлении вредоносного программного кода в автоматическим режиме производится изолирование файла с выявленным вредоносным программным кодом средствами ИС и оповещение специалиста СИБ, который проводит анализ информации.

8. При выявлении критических уязвимостей в ИС производится автоматическое закрытие выявленных уязвимостей, с дальнейшим оповещением пользователей о необходимости перезагрузки оборудования пользователя и/или автоматическая перезагрузка оборудования пользователя в не активный период пользователя для применения обновлений для устранения выявленных уязвимостей в ИС.

9. При выявлении наличия обновлений для ИС производится оповещение специалиста ДИТ для утверждения обновления для ИС, после чего в автоматическом режиме производится установка одобренных обновлений ИС с дальнейшим оповещением пользователей о необходимости перезагрузки оборудования пользователя и/или автоматическая перезагрузка оборудования пользователя в не активный период пользователя для применения обновлений в ИС.

10. По умолчанию пользователю не предоставляются права локальной привилегированной учетной записи на оборудовании пользователя. Права локальной привилегированной учетной записи могут быть предоставлены пользователям СИБ и ДИТ, а также пользователям по согласованию с руководителем Компании, в случаи конфликтной работы ИС.

11. Контроль за установленным ИС на оборудовании пользователей осуществляется специалистом СИБ. Проверки осуществляются выборочно, в произвольном порядке, без предварительного предупреждения, или, при наличии специальной инсталлированной ИС, дистанционно, при помощи консоли управления.

12. На всех ИС в локальной сети обеспечивается синхронизация системного времени с централизованным источником эталонного времени.

3.2 Порядок установки ИС, устанавливаемых на серверах Компании

1. На серверы Компании возможна установка только лицензионного, условно-бесплатного, бесплатного, свободно распространяемого с открытым кодом (GNU) или разработанного в ДИТ ИС.

2. Использование пиратских копий ИС категорически запрещается.

3. Если необходимые ИС приобретены и на них имеются клиентские лицензии, то специалисты ДИТ устанавливают ИС на сервер.

4. Контроль за целостностью ИС на серверах осуществляется постоянно специалистами ДИТ.

3.3 Особенности настроек аудита на оборудовании пользователей и серверах Компании

1. Для получения максимальной информации о событиях на оборудовании пользователей или серверах, рекомендуется включение аудита событий безопасности, системы и приложений.

2. Допускается установка программных брандмауэров на оборудовании пользователей и серверы.

3. Компания обеспечивает ведение журнала аудита в процессе функционирования ИС. Срок хранения аудиторского следа составляет не менее 3 (трех) месяцев в оперативном доступе и не менее 5 (пяти) лет в архивном доступе. В ИС используется функция ведения аудиторского следа, которая отражает формат и информацию, предусмотренную законодательством РК. Хранение аудиторского следа осуществляется на оборудовании пользователей.

3.4 Порядок размещения дистрибутивов ИС на файловых серверах

1. Дистрибутивы ИС размещаются в сетевой папке ДИТ. Размещаемое ИС определяется руководителем ДИТ.
2. Дистрибутивы клиентских частей СУБД, средств реализации SQL-запросов, программ удаленного управления, АРМов и др. располагаются в сетевой папке ДИТ.
3. Пользователи не имеют открытого доступа к дистрибутивам ИС, размещаемых в сетевых папках/сетевых хранилищах.

3.5 Порядок работы с электронно-цифровыми подписями и криптографией

1. Руководитель структурного подразделения формирует и направляет в ДИТ заявку на доступ и установку на оборудование пользователя, специализированного криптографического программного обеспечения, которое устанавливается на оборудовании пользователя и эксплуатируется им для выполнения должностных обязанностей.
2. Для выпуска электронно-цифровой подписи к информационным базам, банк-клиент, государственным ресурсам и базам данных пользователем формируется заявка с обозначением необходимого уровня доступа и визируется руководителем структурного подразделения, с подробным обоснованием служебной необходимости электронно-цифровой подписи к необходимым ИС.
3. Данные электронно-цифровые подписи могут размещаться на сетевых ресурсах Компании или на внешних носителях информации, с обязательным ограничением доступа для неуполномоченных пользователей.
4. При использовании внешнего носителя информации с электронно-цифровой подписью, пользователь при завершении работы с электронно-цифровой подписью обязан извлечь внешний носитель информации и поместить его в запираемый шкаф, тумбочку или сейф.
5. Пользователю запрещена передача электронно-цифровой подписи и внешних носителей информации с электронно-цифровой подписью третьим лицам.

Раздел 4. Доступ в информационные системы

4.1 Порядок доступа в ИС для пользователей

1. Доступ в ИС осуществляется путем идентификации и аутентификации технологической учетной записи пользователя. Идентификация и аутентификация пользователей ИС производится посредством ввода пары «технологическая учетная запись пользователя (идентификатор) - пароль» и/или биометрической и/или криптографической и/или аппаратной аутентификации, которые являются уникальными персонализированными идентификаторами для каждого пользователя.
2. Уровни доступа в ИС определяются и при необходимости пересматриваются путем формирования и внедрения уровней доступа/ролей для обеспечения соответствия прав доступа пользователей в ИС их должностным обязанностям. Совокупность таких ролей представляет собой матрицу доступа в ИС.
3. В зависимости от должности и выполняемых должностных обязанностей пользователя, в Компании устанавливаются разные уровни доступа/роли в ИС:

– доступ на чтение – роль пользователя имеет право просматривать данные ИС, но не имеет права на изменение данных;

– доступ для модификаций - роль пользователя имеет право просматривать и изменять данные в ИС, но не имеет права удалять данные из ИС;

– полный доступ – роль пользователя имеет право просматривать, изменять и удалять записи данных в ИС.

4. Матрица доступа в ИС формируется, периодически пересматривается, актуализируется и поддерживается в актуальном состоянии руководителем ДИТ по мере необходимости, на основании информации, предоставленной руководителями подразделений, в электронной форме или на бумажном носителе.

5. Компания обеспечивает проведение процедур безопасности ИС, в том числе защиту информации ИС от несанкционированного доступа, следующим образом:

– настройки в ИС и оборудовании пользователя должны исключать возможность входа в оборудование пользователя и/или доступа в ИС без авторизации пользователя;

– использование межсетевого экрана (firewall) для защиты сети или отдельных её узлов от несанкционированного доступа в соответствии с заданными правилами;

– ежедневное снятие дампа (резервной копии) базы данных ИС;

– хранения на внешних носителях информации резервной копии в местах, защищенных от внешних факторов (сейф в офисном помещении, сейфовый депозитарий банка, помещение с ограниченным доступом).

4.2 Порядок управления учетными записями пользователей

1. Порядок управления технологическими учетными записями пользователей и паролями, а также блокировке технологических учетных записей пользователей, определяется Компанией и включает функции:

– определение типа учетной записи (технологическая учетная запись, привилегированная учетная запись, временная и (или) иные типы записей);

– объединение технологических учетных записей пользователей в группы (при необходимости);

– верификацию пользователя (проверка личности пользователя, его должностных обязанностей) при создании технологической учетной записи пользователя;

– создание, активация, блокирование и удаление технологических учетных записей пользователя;

– пересмотр и, при необходимости, корректировка технологических учетных записей пользователя;

– порядок заведения и контроля использования временных учетных записей пользователей, а также привилегированных учетных записей;

– оповещение ДИТ, осуществляющего управление технологическими учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;

– удаление/отключение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в ИС;

– предоставление пользователям прав доступа к ИС, основываясь на задачах, решаемых пользователями в ИС и взаимодействующими с ней ИС.

2. Временная учетная запись может быть заведена для пользователя на ограниченный по времени срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (аудиторам, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к ИС).

4.3 Порядок по управлению паролями и блокировками учетных записей пользователей

1. В ИС применяются следующие параметры функции по управлению паролями и блокировками учетных записей пользователей:

– минимальная длина пароля - значение данного параметра составляет не менее 8 символов. Проверка пароля на соответствие данному параметру производится при каждой смене пароля, в случае несоответствия - выдается уведомление пользователю;

– сложность пароля - возможность проверки наличия в пароле, как минимум трех групп символов: строчных букв, заглавных букв, цифровых значений, специальных символов.

Проверка пароля на соответствие данному параметру производится при каждой смене пароля, в случае несоответствия - выдается уведомление пользователю;

– история пароля - новый пароль не повторяет как минимум семь предыдущих паролей. Проверка пароля на соответствие данному параметру производится при каждой смене пароля, в случае несоответствия выдается уведомление пользователю;

– минимальный срок действия пароля - 1 (один) рабочий день;

– максимальный срок действия пароля - не более 60 (шестидесяти) календарных дней. Проверка пароля на соответствие данному параметру производится при каждом входе в ИС и смене пароля. По истечении максимального срока действия пароля ИС блокирует доступ и требует обязательную смену пароля;

– при первом входе в ИС, либо после смены пароля привилегированной учетной записью, ИС запрашивает у пользователя смену пароля с невозможностью отклонить данную процедуру. Данное правило превалирует над правилом о сроке действия пароля;

– в случае отсутствия активности пользователя в ИС более 30 (тридцати) календарных дней его технологическая учетная запись пользователя автоматически блокируется;

– при последовательном пятикратном вводе неправильного пароля технологическая учетная запись пользователя временно блокируется;

– при неактивности пользователя более 30 (тридцати) минут ИС автоматически завершает сеанс работы пользователя либо блокирует оборудование пользователя с возможностью разблокировки только при вводе данных для авторизации пользователя.

4.4 Порядок использования привилегированных учетных записей пользователей

1. Перечень привилегированных учетных записей формируется руководителем ДИТ в электронной форме или на бумажном носителе, который актуализируется и поддерживается в актуальном состоянии руководителем ДИТ по мере необходимости, на основании используемых ИС.
2. Доступ к привилегированным учетным записям имеют только сотрудники ДИТ.
3. Ведение двойного контроля при использовании функций администрирования ИС осуществляется посредством согласования заявки на создание\изменение учетных записей ИС. Процесс согласования включает в себя следующие этапы:

- формирование руководителем подразделения соответствующей заявки;
- согласование заявки со стороны СИБ (согласовано, отказано);
- исполнение заявки ДИТ.

4.5 Порядок доступа к ИС для сотрудников сторонних организаций (третьи лица)

1. При подписании договора со сторонней организацией на оказание технической поддержки, разработки/обновления/внедрения ИС, определенному сотруднику сторонней организации ДИТ предоставляет доступ к ИС на период и в объеме, определяемый договором (проводимыми работами) с условием о соблюдении им требований к информационной безопасности, за исключением случаев, предусмотренных законодательством.
2. При этом, договор со сторонней организацией должен содержать: обязанность об обеспечении обновлений безопасности ИС, положение о конфиденциальности, ответственность с возмещением ущерба, возникшего вследствие нарушения информационной безопасности, а также сбоев в работе ИС и нарушении их безопасности, вызванных действием или бездействием сотрудником сторонней организации, а также условие о возложении ответственности за действия сотрудников сторонних организаций в ИС - на самих сотрудников данных организаций в полном объеме.
3. Для сотрудников сторонней организации, согласно договору, Компания предоставляет доступ к ИС, находящимся внутри периметра защиты, при подключении из-за пределов периметра защиты по зашифрованному каналу с аутентификацией пользователя на периметре защиты.
4. Разработка, доработка, поддержка и обслуживание ИС не осуществляется в среде промышленной эксплуатации и осуществляется сотрудниками сторонних организаций, предоставляющих перечисленные услуги.

5. Сотрудники сторонних организаций, осуществляющие разработку, доработку ИС в тестовой среде не осуществляют перенос обновлений и/или изменений для ИС и не имеют доступ к ИС в промышленной среде. Обновления и/или изменения для ИС до переноса и внедрения в промышленную среду проходят испытания в тестовой среде. Перенос и внедрение прошедших тестирование в тестовой среде обновлений и/или изменений для ИС осуществляется с помощью подготовленных пакетов обновлений исключительно сотрудниками ДИТ. СИБ проводят предварительную контрольную проверку пакетов обновлений для ИС.
Пакеты обновлений и/или изменений могут содержать: обновлений безопасности ИС, обновление существующих функций ИС, обновления, связанные с новыми функциями ИС.
Пакеты обновлений не могут содержать обновления и/или изменения, затрагивающие непосредственно данные (записи), а также изменять уровень прав доступа в промышленной среде ИС.

6. При предоставлении доступа авторизованным третьим лицам к ИС, СИБ осуществляет анализ рисков информационной безопасности и при необходимости разрабатывает мероприятия по снижению выявленных рисков.

7. Компания использует доступные методы, исключающие доступ не авторизованных третьих лиц к информации, передача которой не авторизованным третьим лицам не допускается в соответствии с законодательством РК.

Методы защиты оборудования и ИС от несанкционированного доступа делятся на программно-аппаратные и технические. Первые отсекают неавторизованных пользователей, вторые предназначены для исключения физического проникновения посторонних людей в помещения Компании, среди которых:

- аутентификация и идентификация при входе в ИС;
- контроль уровней допуска в ИС для пользователей;
- обнаружение и регистрация попыток несанкционированного доступа в ИС;
- контроль непрерывности функционирования ИС;
- обеспечение безопасности во время профилактических или ремонтных работ;
- ограничение несанкционированного доступа в помещения Компании пользователей и третьих лиц.

Для методов защиты информации от несанкционированного доступа предусмотрено 4 этапа:

- предотвращение – профилактические меры, ограничение доступа неавторизованным пользователям и третьим лицам;
- обнаружение – комплекс действий, предпринимаемых для выявления злоупотреблений;
- ограничение – механизм снижения потерь, если предыдущие меры удалось обойти;
- восстановление – реконструкция ИС, которая производится по программе/плану восстановления ИС.

8. При предоставлении клиентам Компании доступа к ИС в рамках заключенных с ними договоров, доступ к ИС предоставляется только авторизованным клиентам в необходимом объеме, с определением и соблюдением мер информационной безопасности.

Раздел 5. Подключение к локальной сети и предоставление сетевых каталогов пользователям. Удаленное управление оборудованием.

5.1 Подключение к локальной сети и предоставление сетевых каталогов пользователям

1. Сетевое имя оборудования пользователя должно соответствовать инвентарному номеру оборудования. Для сетевых имен серверов необходимо использовать произвольное буквенное сокращение, не обозначающее назначение сервера.

2. Каждому структурному подразделению присваивается диапазон IP адресов. Учет и присвоение IP адресов производится специалистами ДИТ.

3. Подключение рабочего места пользователя к локальной сети Компании и получение адреса корпоративной электронной почты осуществляются по заявке от руководителя структурного подразделения.

4. Организационно-технические мероприятия по подключению оборудования пользователя к ИС локальной сети осуществляются специалистом ДИТ. Данные мероприятия включат в себя

настройку сетевой платы оборудования пользователя с назначением IP адреса для оборудования пользователя, предоставление адреса корпоративной электронной почты, предоставление доступа к каталогам структурных подразделений на файловом сервере, регистрацию пользователя в ИС.

5. ДИТ вносит все изменения в структуре сети в электронный файл, отображающий топологию локальной сети Компании.

6. Настройки в ИС и оборудовании пользователя должны исключать возможность локального входа в оборудование пользователя и/или доступа к сетевым ресурсам без авторизации пользователя в ИС.

5.2 Удаленное (дистанционное) управление серверами, активным сетевым оборудованием и оборудованием пользователя

1. Удаленное (дистанционное) управление оборудованием из внешней сети разрешается только при использовании шифрованных выделенных виртуальных каналов (VPN).

2. Правила работы в дистанционном режиме для пользователей:

– в Компании исключается возможность использования для работы в дистанционном режиме пользователями подключения к локальной сети с открытых Wi-Fi-сетей, в которых возможен перехват трафика;

– домашние Wi-Fi-сети пользователей должны быть защищены паролями и шифрованием как минимум уровня WPA2;

– подключение оборудования пользователей для работы в дистанционном режиме к локальной сети должно происходить только по каналам VPN с авторизацией пользователя на периметре защиты. При необходимости, Компания предоставляет пользователю отдельное оборудование пользователя для работы в дистанционном режиме. На оборудовании пользователя для работы в дистанционном режиме специалистами ДИТ устанавливаются необходимые ИС и клиент ИС для безопасного подключения к локальной сети по каналу VPN;

– сведения о работе в дистанционном режиме не должны публиковаться в социальных сетях, чтобы не вызвать интерес злоумышленников. Устное и письменное разглашение конфиденциальных данных пользователем недопустимо;

– пароли от ИС, связанные с работой в дистанционном режиме, пользователю необходимо регулярно менять, согласно требованиям настоящих Правил;

– ИС на оборудование пользователя для работы в дистанционном режиме должны регулярно обновляться специалистами ДИТ;

– доступ на оборудование пользователя для работы в дистанционном режиме в обязательном порядке должен производится только после авторизации пользователя посредством логина и пароля;

– при дистанционном режиме работы доступ к ИС предоставляется в необходимом объеме, с определением и соблюдением мер информационной безопасности.

3. При подключении пользователей к ИС из-за пределов периметра защиты, Компания применяет методы двухфакторной аутентификации с аутентификацией пользователя на периметре защиты.

Раздел 6. Оборудование

6.1 Порядок закрепления оборудования пользователя

1. Оборудования пользователя закрепляется за пользователем при зачислении на штатную должность, в соответствии с заявкой, подаваемой руководителем структурного подразделения в ДИТ. Затем пользователь получает в ДИТ оборудование, с отключенными/заблокированными портами ввода-вывода и дисководом (при наличии). Факт возврата оборудования пользователями при их увольнении подтверждается подписью сотрудника ДИТ в обходном листе уволившегося пользователя.

2. На оборудовании пользователя должны быть установлены необходимые ИС для выполнения должностных обязанностей, а также антивирусное программное обеспечение.

3. Специалистом ДИТ в целях безопасности на оборудовании пользователя устанавливается клиентская часть специализированной ИС, позволяющей централизованно

контролировать состояние настроек, аппаратную конфигурацию и целостность программного обеспечения.

4. После установки оборудования пользователя на рабочее место, специалистом ДИТ пользователю предоставляются одноразовые пароли в ИС с дальнейшей их сменой пользователем.

5. Оборудование пользователя подлежит пломбированию перед установкой его на рабочее место пользователя. Пользователю запрещается вскрывать оборудование пользователя, производить какие-либо изменения в аппаратной конфигурации и самостоятельно подключать к оборудованию пользователя периферийного оборудования.

6. В Компании осуществляется видеоконтроль перемещения оборудования пользователя, периферийного оборудования и носителей информации через границу физического периметра безопасности.

6.2 Ремонт оборудования пользователя

1. В случае возникновения технических неисправностей оборудовании пользователя пользователь направляет в ДИТ запрос в произвольной форме, в электронном или бумажном виде. Перенос конфиденциальной информации с неисправного оборудования пользователя возлагается на специалистов ДИТ.

2. В случае необходимости проведения ремонтных работ, смены или замены комплектующих, подключения/отключения периферийных устройств на оборудовании пользователя, специалистом ДИТ проверяется целостность пломб в присутствии лица, за которым было закреплено оборудование пользователя. Затем оборудование пользователя вскрывают, проводят необходимые работы. После выполнения ремонтных работ оборудование пользователя пломбируется специалистами ДИТ.

3. В случае выполнения ремонтных работ в сторонних организациях информация на носителях информации с оборудования пользователя в обязательном порядке переносится на сетевой ресурс и/или резервируется на внешний носитель информации, после чего носители информации с оборудования пользователя форматируются.

4. В случае если на оборудовании пользователя вышел из строя носитель информации - специалисты ДИТ пытаются восстановить информацию и перенести данные на сетевой ресурс, внешний носитель информации. После чего, специалисты ДИТ списывают вышедший из строя носитель информации с последующим его уничтожением в установленном порядке.

6.3 Порядок использования периферийного оборудования

1. Для подключения/предоставления периферийного оборудования пользователем подается заявка в ДИТ, с подробным обоснованием служебной необходимости и сроком использования в работе периферийного оборудования.

2. Периферийное оборудование должно использоваться пользователем только в соответствии с обоснованием, указанным в заявке на подключение данного оборудования.

3. По истечении срока использования периферийного оборудования, указанного в заявке, оборудование отключается/изымается сотрудником ДИТ.

4. Несанкционированное использование периферийного оборудования, в том числе личного оборудования, в локальной сети Компании запрещается.

6.4 Порядок закрепления сервера за администратором сервера

1. Сервер закрепляется при вводе его в эксплуатацию за администратором сервера и указывается в паспорте сервера.

2. При прекращении (расторжении) трудового договора или переводе на другую должность администратора сервера, составляется акт приема-передачи сервера. Все пароли доступа изменяются новым администратором сервера.

3. На серверы устанавливается клиентская часть специализированного ПО, позволяющего централизованно контролировать состояние настроек, аппаратную конфигурацию и целостность программного обеспечения.

6.5 Паспортизация и пломбирование серверов

1. Серверы подлежат паспортизации после завершения настроек, инсталляции ИС и введения его в эксплуатацию, о чем в паспорт сервера вносится соответствующая запись. Паспорт сервера заполняется специалистом ДИТ - администратором сервера. Паспорт сервера хранится в ДИТ.

2. Паспорт сервера составляется при вводе в эксплуатацию, и содержит информацию о:

- технических характеристиках сервера;
- подключенных к нему периферийных устройствах;
- проведенных ремонтах в процессе эксплуатации;
- месте установки сервера;
- сетевого имени сервера;
- IP адреса сервера и перечень IP адресов оборудования пользователей, с которых возможно удаленное управление сервером;
- перечень открытых портов и назначение сервисов, работающих на этих портах;
- перечень установленных на данном сервере ИС, сведения о клиентских лицензиях на ИС;
- сведения о закреплении сервера за конкретным администратором сервера;
- системном пароле сервера.

3. В ходе эксплуатации сервера в паспорт сервера специалистом ДИТ - администратором сервера вносятся пометки об изменении информация связанной:

- с изменением периферийного оборудования;
- со сменой администратора сервера и системного пароля сервера;
- с изменением перечня открытых портов и назначение сервисов, работающих на этих портах;
- с изменением перечня IP адресов оборудования пользователей, с которых возможно удаленное управление сервером;
- с изменением перечня ИС и сведений о клиентских лицензиях на ИС;
- с заменой/добавлением блоков сервера в ходе устранения неисправностей и/или модернизацией сервера.

4. Пломбирование сервера осуществляется при необходимости специалистами ДИТ специальными пломбами.

6.6 Ремонт серверов

1. В случае возникновения технических неисправностей сервера, контроль за переносом конфиденциальной информации с неисправного сервера возлагается на специалиста ДИТ - администратора сервера.

2. В случае необходимости проведения ремонтных работ, смены или замены комплектующих, подключения/отключения периферийных устройств сервера, специалистами ДИТ проверяется целостность пломб. Затем сервер вскрывается и проводятся необходимые работы. После выполнения ремонтных работ сервер пломбируется специалистами ДИТ.

3. В случае выполнения ремонтных работ в сторонних организациях информация на носителях информации сервера в обязательном порядке переносится на резервный сервер и/или резервируется на внешний носитель информации, после чего носители информации сервера форматируются.

4. В случае если на сервере из строя вышел носитель информации - специалист ДИТ пытается восстановить информацию и перенести данные на внешний/резервный носитель информации. После чего, специалисты ДИТ списывают вышедший из строя носитель информации с последующим его уничтожением в установленном порядке.

Раздел 7. Инструкция по резервному копированию, хранению, архивированию, восстановлению ИС. Тестирование планов восстановления ИС.

7.1 Инструкция по резервному копированию и восстановлению

1. Резервное копирование ИС предназначено для решения задач по восстановлению информации в случаях, связанных с повреждением или уничтожением информации в ИС и

тестированию планов восстановления ИС. Компания обеспечивает резервное копирование и хранение актуальных резервных копий ИС, включающие в себя данные, файлы и настройки ИС.

2. Резервному копированию в обязательном порядке подлежат:

– конфиденциальные данные в ИС;

– юридически важные документы, хранящиеся в электронном виде;

– данные системы, без которых невозможна ее нормальная работа ИС;

– прочие важные данные, которые записаны на физически ненадежных носителях информации и носителях, поддерживающих операции перезаписи;

– данные на ресурсах сети общего пользования;

– другие данные согласно решению руководителя Компании.

3. Резервное копирование производится технологиями RAID массивов, копированием данных в реальном времени на резервные сервера, а также на внешние носители информации или сетевые ресурсы.

4. Еженедельно последние актуальные резервные копии переносятся с сетевых ресурсов на внешние носители информации (ВНИ-1), текущий внешние носители информации (ВНИ-1), подлежат переносу в огнеупорный сейф на период хранения, а внешние носители информации (ВНИ-2), находившиеся в сейфе, подлежат отправке в банковскую сейфовую ячейку (защищенный депозитарий). Внешние носители информации (ВНИ-3), который до этого момента находился в банковской сейфовой ячейке размещается в серверной для ежедневного сохранения актуальных резервных копии ИС. По завершению периода хранения (6 - 10 дней) цикл повторяется.

5. Защищенный депозитарий, в котором хранятся актуальные резервные копии ИС, обеспечивает возможность своевременного восстановления работоспособности ИС.

6. Операция резервного копирования для хранения актуальных резервных копий ИС, ведется в виде, обеспечивающем возможность своевременного восстановления работоспособности ИС с сохранением на внешних носителях информации или сетевых ресурсах и производится по окончанию каждого рабочего дня.

7. В целях обеспечения непрерывности функционирования ИС в Компании предусмотрена и утверждена программа/план восстановления ИС в случае частичного или полного ее разрушения:

Восстанавливаемые ИС и оборудование	Возможные сценарии/причины/критерии внештатной ситуации	Действия команды восстановления/план/подходы восстановления	Требования по срокам и месту проведения работ
Серверное оборудование	Вышел из строя один или несколько компонентов сервера	ремонт неисправных компонентов и/или замена неисправных компонентов сервера (если ремонт невозможен)	до 5 рабочих дней, в офисном помещении
	Вышел из строя основной компонент сервера или произошло полное разрушение сервера	полная замена/замещение вышедшего из строя сервера (если ремонт невозможен) другим сервером с последующим восстановлением ИС из актуальной резервной копии	до 20 рабочих дней, в офисном помещении
	Обесточивание сервера (отключение основной линии питания)	система автоматически переходит к питанию с ИБП либо на резервную линию питания	моментально, в офисном помещении

Оборудование пользователя	Вышел из строя один или несколько компонентов оборудования пользователя	ремонт неисправных компонентов и/или замена неисправных компонентов оборудования пользователя (если ремонт невозможен)	до 5 рабочих дней, в офисном помещении
	Вышел из строя основной компонент оборудования пользователя или произошло полное разрушение оборудования пользователя	полная замена оборудования пользователя с последующим восстановлением/переносом с носителей информации данных пользователя (при возможности восстановления)	до 5 рабочих дней, в офисном помещении
	Обесточивание оборудования пользователя (отключение основной линии питания)	система автоматически переходит к питанию с ИБП либо на резервную линию питания (при наличии)	моментально, в офисном помещении
Коммутационное оборудование	Вышел из строя один или несколько компонентов коммутационного оборудования	ремонт неисправного компонента и/или замена неисправного компонента коммутационного оборудования (если ремонт невозможен)	до 5 рабочих дней, в офисном помещении
	Вышел из строя основной из компонентов коммутационного оборудования или произошло полное разрушение коммутационного оборудования	переход на резервное коммутационное оборудование	до 20 минут, в офисном помещении
	Полное разрушение локальной сети	1. установка «прямого» подключения сервера с оборудованием пользователя 2. после устранения сбоя восстановление подключения через коммутационное оборудование	до 7 рабочих дней, в офисном помещении
	Обесточивание коммутационного оборудования (отключение основной линии питания)	система автоматически переходит к питанию с ИБП либо на резервную линию питания	моментально, в офисном помещении
Информационная система (Перечень ИС, подлежащих восстановлению, формируется руководителем ДИТ в электронном или бумажном виде, который им актуализируется и поддерживается в актуальном состоянии по мере необходимости, на основании используемых ИС)	Сбой в исполняемых модулях ИС	1. восстановление исполняемых модулях ИС с актуальной резервной копии; 2. отправление разработчикам отчетов и логов ИС для выявления и устранения причины сбоя	до 2 рабочих дней, в офисном помещении
	Сбой, связанный с повреждением или уничтожением информации в ИС	1. восстановление информации в ИС с актуальной резервной копии; 2. отправление разработчикам отчетов и логов ИС для выявления и устранения причины сбоя	до 2 рабочих дней, в офисном помещении
	Вышла из строя ИС или полный ее сбой	1. полное восстановление ИС с актуальной резервной копии;	до 3 рабочих дней, в офисном

		2. по возможности отправление разработчикам отчетов и логов ИС для выявления и устранения причины сбоя	помещении

8. В целях поддержания работоспособности ИС по заключению и исполнению сделок с ценными бумагами, а также по учету активов компании и клиентов в случаях отключения электропитания и исчезновения (недостатка) других ресурсов, используемых для работы указанных систем в обычном режиме, Компания использует блоки бесперебойного питания и закрепляет администратора сервера, который обеспечивает при экстремальных ситуациях немедленное сохранение данных с одновременным созданием актуальных резервных копий на носителях информации.

9. Восстановление информации из актуальных резервных копий производится и контролируется специалистами ДИТ. Решения о восстановлении ИС принимаются руководителем ответственного подразделения при обнаружении случая повреждения или уничтожения информации в ИС и производится после согласования с руководителем Компании.

10. Для восстановления ИС при наступлении форс-мажорных обстоятельств и стихийных бедствий специалистами ДИТ осуществляются следующие действия:

- анализ и выявление разрушений/сбоев в оборудовании и ИС;
- устранение причины разрушения/сбоя самостоятельно и восстановление работоспособности оборудования и ИС при возможности;
- при отсутствии возможности устранения причины разрушения/сбоя самостоятельно - обращение к поставщику или в специализированную организацию за консультацией и помощью;
- использование резервного сервера/оборудования (при наличии) для временного поддержания работоспособности ИС;
- восстановление данных из актуальной резервной копии при необходимости.

7.2 Тестирование программы/плана восстановления ИС из резервных копий

1. В целях проверки готовности процессов восстановления деятельности ИС Компания проводит тестирование восстановления ИС из резервных копий в соответствии с программой/планом восстановления, не менее одного раза в год (далее - тестирование программы/плана восстановления).

2. Тестирование планов восстановления ИС проводится по разработанной и утвержденной программе/плану, предусматривающей описание восстанавливаемых ИС и оборудования, возможных сценариев/причин/критериев внештатной ситуации, действий команды восстановления/планов/подходов восстановления, требований по срокам и месту проведения работ.

3. По итогам тестирования планов восстановления ИС подготавливается протокол о результатах тестирования с указанием:

- перечня ИС, по которым проведено тестирование;
- времени, затраченного на восстановление работы ИС;
- выявленных недостатков планов восстановления и предложений по их устранению.

Раздел 8. Защищаемая информация

8.1. Перечень защищаемой информации

1. К защищаемой информации относится конфиденциальная информация, содержащая инсайдерскую и коммерческую тайну на рынке ценных бумаг, предусмотренную настоящими Правилами и законодательством РК. Таким образом, под защищаемой информацией понимают сведения, использование и распространение которых ограничены их собственниками, т.е. субъектами информационных отношений.

2. Защищаемую информацию на рынке ценных бумаг составляет информация о наличии лицевого счета в системе учета центрального депозитария и номинального держания, о наличии, остатках, движении и владельцах эмиссионных ценных бумаг и других финансовых инструментов на лицевых счетах в системе учета центрального депозитария и номинального держания, за исключением сведений о крупных акционерах эмитента и количестве принадлежащих им акций данного эмитента, об эмитенте и остатках эмиссионных ценных бумаг на лицевых счетах эмитента по учету объявленных эмиссионных ценных бумаг и по учету выкупленных эмиссионных ценных бумаг в системе учета номинального держания и (или) системе учета центрального депозитария. Компания не вправе разглашать данную информацию и допускать действия, которые могут повлечь нарушение естественного ценообразования и дестабилизацию рынка ценных бумаг.

Защищаемой информацией также является: штатное расписание и заработная плата работников; сведения о работниках Компании, включая персональные данные работников, сведения из личного дела; информация о подготовке, принятии и исполнении отдельных решений руководителем Компании по производственным, организационным и иным вопросам; о совещаниях: целях, рассматриваемых вопросах, результатах, фактах проведения совещаний и заседаний органов управления Компанией; о проектах и действующих договорах, об организации и состоянии ИС, инвестиционные решения, данные бухгалтерского учета; о текущем финансовом состоянии Компании; о финансовых планах Компании; информация о партнерах Компании, предоставленная партнерами на доверительной основе, о применяемых Компанией оригинальных методах изучения рынка; имена клиентов, держателей паев инвестиционных фондов, количество паев и акций, принадлежащих держателям паев и акционерам, объем произведенных ими инвестиций, наименование фондов, вкладчиками которых они являются; содержание принятых решений в рамках брокерско-дилерской деятельности и деятельности по управлению инвестиционным портфелем; данные клиентских заказов; структура инвестиционного портфеля клиентов и фондов; персональные данные клиентов.

**Персональные данные по доступности подразделяются на общедоступные и ограниченного доступа:* Общедоступные персональные данные - персональные данные, доступ к которым является свободным с согласия субъекта или на которые в соответствии с законодательством РК не распространяются требования соблюдения конфиденциальности. В целях информационного обеспечения населения используются общедоступные источники персональных данных (в том числе биографические справочники, телефонные, адресные книги, общедоступные электронные информационные ресурсы, средства массовой информации).

Персональные данные ограниченного доступа - персональные данные, доступ к которым ограничен законодательством Республики Казахстан. К ним относятся установочные данные лица (фамилия, имя, отчества, год, дата рождения, национальность), сведения о месте жительства (место регистрации), индивидуальном идентификационном номере (ИИН), документах, удостоверяющих личность (номер), дактилоскопическая и геномная информация и другие сведения.

3. Если информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, то Компания принимает меры к охране ее конфиденциальности и недопущению ее использования в собственных интересах, работников или третьих лиц.

4. Обобщенная информация, не раскрывающая сведений о конкретном субъекте, является общедоступной и не является информацией, составляющей защищаемую информацию, также как и сведения об аффилированных лицах Компании.

5. Компания обеспечивает запись, сохранность, конфиденциальность и неизменность информации, получаемой и передаваемой через корпоративные средства связи, а также обеспечивает хранение данной информации в течение пяти лет.

8.2. Раскрытие защищаемой информации

1. Сведения, составляющие защищаемую информацию, не подлежат разглашению, за исключением случаев, установленных законодательством РК, т.е. представляются только органам, организациям, учреждениям и лицам, прямо предусмотренным законодательством РК.

2. Запрещается копирование и размножение такой информации, кроме как, в случаях, предусмотренных внутренними документами Компании и в случаях, установленных законодательством РК.

8.3. Доступ к защищаемой информации

1. Полным доступом к защищаемой информации обладает первый руководитель Компании или лицо, исполняющее его обязанности, а также специалисты ДИТ и СИБ.

2. Доступ пользователей к защищаемой информации определяется должностными обязанностями пользователей. Определение круга лиц внутри структурного подразделения, имеющих доступ к защищаемой информации, степени их осведомленности, а также порядок циркуляции этой информации между структурными подразделениями возлагается на руководителя соответствующего структурного подразделения.

8.4. Порядок уничтожения защищаемой информации

1. Уничтожение защищаемой информации производится на основании служебной записки от специалиста ДИТ и осуществляется после ее согласования с руководителем Компании.

2. Уничтожение защищаемой информации производится методами, исключающими ее восстановление, с использованием любого из следующих методов гарантированного уничтожения информации в зависимости от типа носителя:

- физическое уничтожение носителя информации;
- электромагнитное воздействие на носитель информации (для магнитных носителей);
- программное уничтожение электронной информации специализированными программными средствами.

3. После уничтожения защищаемой информации специалистом ДИТ составляется Акт об уничтожении защищаемой информации, который подписывается комиссией (руководитель Компании или его заместитель, юрист и руководитель ответственного подразделения).

4. Служебная записка и Акт об уничтожении защищаемой информации хранятся в ДИТ.

8.5. Ответственность за разглашение защищаемой информации

1. Компания обязана обеспечивать соблюдение условий, позволяющих предотвратить использование сведений, которые составляют защищаемую информацию. Все работники подписывают обязательство о неразглашении информации, составляющей защищаемую информацию с предупреждением об ответственности за ее разглашение, при этом, передача третьим лицам, публикация без согласия Компании, а также использование для занятия любой деятельностью, которая может нанести ущерб Компании, влечет ответственность в соответствии с законодательством РК.

2. За разглашение защищаемой информации работник может быть освобожден от занимаемой должности с предъявлением ему требований о возмещении причиненного ущерба. Срок действия ограничений, связанных с необходимостью защиты защищаемой информации, начинается с момента заключения трудового договора. Увольнение из Компании не освобождает работника от ответственности за разглашение защищаемой информации, при этом установленные ограничения распространяются на срок, предусмотренный законодательством РК.

Раздел 9 Оценка компетенций руководителя СИБ

1. Оценка компетенций Руководителя СИБ осуществляется в соответствии с Требованиями к компетенциям руководителей и работников подразделений информационной безопасности, включая требования по повышению квалификации лиц, ответственных за обеспечение информационной безопасности, утвержденных Постановлением №89 от 21 сентября 2020 года (далее - Требования).

2. Оценка компетенций Руководителя СИБ осуществляется при приеме либо при переводе работника Компании на должность Руководителя СИБ.

3. Оценка компетенций Руководителя СИБ включает в себя соответствие руководителя Требованиям, в части:

- наличия высшего образования;
- наличия опыта работа не менее 3-х лет по одному из доменов Требований;
- наличия сертификата согласно пп.4 п. 18 Требований;
- соответствия опыта работы задачам, возложенным на СИБ.

4. Оценка компетенций Руководителя СИБ осуществляется курирующим СИБ членом Правления. Результат оценки оформляется в соответствии с Приложением 1.

Приложение 1.

Оценка компетенций Руководителя Службы информационной безопасности.

ФИО руководителя	
Образование	
Опыт работы	
Курсы\Сертификаты	
Дополнительные сведения	
Оценка компетенции (соответствует\ не соответствует)	

Дата:_____

ФИО куратора:_____

Подпись:_____