УТВЕРЖДЕНА
приказом Генерального директора
ТОО «Қамқор Менеджмент»
от «_27_»_марта_ 20_18_ года
№_АЦК-016_

ПОЛИТИКА
информационной безопасности товарищества с ограниченной ответственностью «Қамқор Менеджмент»

г. Астана - 2018 год

Содержание

1. Назначение

Настоящая Политика информационной безопасности (далее - Политика) разработана с целью определения стратегических целей, задач и основных требований к комплексу мер в области обеспечения информационной безопасности, принимаемых в товариществе с ограниченной ответственностью «Қамқор Менеджмент» (далее - Товарищество).

Информация является ценным активом Товарищества.

Использование информационных систем, внутренней локально-вычислительной сети и глобальной сети Интернет для поиска, передачи, хранения, обработки и анализа информации позволяет повысить эффективность работы Товарищества.

Однако, использование информационных ресурсов ненадлежащим образом может подвергнуть Товарищество к значительным рискам, нанести ущерб репутации, финансовый, материальный или нематериальный ущерб.

Все работники, и другие лица, допущенные к информационным ресурсам Товарищества, несут ответственность за бережное и рациональное использование информации и соблюдение требований настоящей Политики.

Доступ к информационным ресурсам Товарищества предоставляется только после ознакомления с настоящей Политикой и подписания работником Товарищества обязательства о неразглашении документов и сведений, составляющих защищаемую информацию.

Основной целью, на достижение которой направлены все процедуры информационной безопасности, является минимизация ущерба от событий, представляющих угрозу безопасности информации, посредством их предотвращения или сведения их последствий к минимуму.

Обеспечение информационной безопасности необходимо для снижения рисков и экономических потерь, связанных со всевозможными угрозами имеющимся информационным ресурсам Товарищества.

Настоящая Политика разработана в соответствии с требованиями стандартов ИСО 9001:2016 «Системы менеджмента качества», сертифицированных в Товариществе (Ссылка №1), а также ISO 27001:2013 «Информационные технологии - Методы обеспечения безопасности - Системы управления информационной безопасностью - Требования» (Ссылка №2).

2. Область применения

В Казахстане действует Концепция информационной безопасности (далее – Концепция). Концепция выражает совокупность официальных взглядов на сущность и содержание деятельности Республики Казахстан по обеспечению информационной безопасности государства и общества, их защите от внутренних и внешних угроз. Концепция определяет задачи,

приоритеты, направления и ожидаемые результаты в области обеспечения информационной безопасности личности, общества и государства. Она является основой для конструктивного взаимодействия органов государственной власти, бизнеса и общественных объединений для защиты национальных интересов Республики Казахстан в информационной сфере.

Концепция призвана обеспечить единство подходов к формированию и реализации государственной политики обеспечения информационной безопасности, а также методологическую основу для совершенствования нормативных правовых актов, регулирующих данную сферу.

Настоящая Политика разработана в соответствии с концепцией, предусмотренной Законом Республики Казахстан «О национальной безопасности**».**

Также, на территории Республики Казахстан действует Закон «О доступе к информации» и распространяется на общественные отношения, связанные с доступом к информации, не относящейся к информации с ограниченным доступом. При этом закон имеет ограниченную сферу действия. Во-первых**,** действие Закона Республики Казахстан «О доступе к информации» не распространяется на обращения физических и юридических лиц, порядок рассмотрения которых установлен законодательством Республики Казахстан об административных правонарушениях, уголовно-процессуальным, гражданским процессуальным законодательством Республики Казахстан. Во-вторых**,** действие закона не распространяется на порядок рассмотрения запросов, установленный Законом Республики Казахстан «О Национальном архивном фонде и архивах». Третье исключение – действие закона не распространяется на порядок предоставления информации средствам массовой информации, предусмотренный Законом Республики Казахстан «О средствах массовой информации».

Способы распространения информации согласно Закону Республики Казахстан «О доступе к информации»:

1) размещение информации на интернет-ресурсах; в средствах массовой информации; в помещениях, занимаемых обладателями информации; размещением информации на веб-портале «Электронное правительство»;
2) другие способы обеспечения права на доступ к информации, предусмотренные законом – обеспечение доступа к информации лицами, обладающими информацией;
3) предоставление информации по запросу – еще один из способов обеспечения права на доступ к информации. Наличие этого способа подразумевает, что пользователь, не найдя нужной информации в

открытых источниках, специально запрашивает ее у обладателя информации.

Действие настоящей Политики распространяется на всех работников Товарищества. Процедуры информационной безопасности учитывают ожидания всех заинтересованных сторон и обязательны для исполнения всеми работниками Товарищества, а также доводятся до сведения клиентов и иных третьих лиц, имеющих доступ к информационным системам и документам Товарищества, в той части, которая непосредственно взаимосвязана с Товариществом и его деятельностью.

Настоящая Политика является документом, доступным любому работнику Товарищества и пользователю его ресурсов, и представляет собой официально принятую руководством Товарищества систему взглядов на проблему обеспечения информационной безопасности, и устанавливает принципы построения системы управления информационной безопасностью на основе систематизированного изложения целей, процессов и процедур информационной безопасности Товарищества.

Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

3. Термины и определения

Защищаемая информация – информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством и внутренними нормативными документами Товарищества к коммерческой, служебной или иной охраняемой законом тайне.

СИТ – Служба информационных технологий Товарищества.

Служба контроля – Служба контроля Товарищества.

Юридическая служба – Служба правового обеспечения Товарищества.

Локально-вычислительная сеть - коммуникационная система, состоящая из определенного количества персональных компьютеров, соединенных между собой посредством кабелей (UTP, FTP, STP, коаксиальный кабель, телефонные линии, радиоканалы и т.д.), позволяющая пользователям совместно использовать ресурсы компьютера: программы, файлы, папки, а также периферийные устройства: принтеры, плоттеры, диски, модемы и т.д.

Рабочая станция - это компьютер, который включен в состав локально-вычислительной сети.

Пользователь – работник Товарищества, использующий рабочую станцию и локально-вычислительную сеть Товарищества для выполнения своих должностных обязанностей.

Информационные системы - системы, предназначенные для хранения, поиска и обработки информации, и соответствующие

организационные ресурсы, которые обеспечивают и распространяют информацию.

Информационные ресурсы - документы и массивы документов в информационных системах.

СЭД - система электронного документооборота, компьютерная система (или набор компьютерных программ), используемая для отслеживания и хранения электронных документов и/или образов (изображений и иных артефактов) бумажных документов.

ЭЦП - электронная цифровая подпись, реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

ПО - программное обеспечение, совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

Стандартное ПО - ПО, включающее в себя:

- операционную систему (Microsoft Windows 7, 8, 8.1, 10 и все последующие версии);
- комплект актуальных драйверов устройств;
- комплект актуальных обновлений для операционных систем Microsoft Windows;
- комплект офисных программ (Microsoft Office 2010, 2013, 2016 и все последующие версии);
- программу для просмотра электронных публикаций в формате PDF (Adobe Reader);
- антивирусное ПО с набором актуальных антивирусных баз;
- личный кабинет СЭД;
- личный ящик корпоративной электронной почты kamkor.org (посредством почтового клиента Microsoft Outlook).

Мультимедиа-контент - услуга, позволяющая получать, просматривать либо воспроизводить на рабочей станции различные медиа-элементы - мелодии всех форматов, реалтоны, видео-ролики и полнометражные фильмы всех форматов, цветные и анимационные картинки, хранители экрана (часы), игры и java-приложения, а также развлекательную информацию различного характера.

СЭА - система электронного архива, система структурированного хранения электронных документов, обеспечивающая надежность хранения,

конфиденциальность и разграничение прав доступа, отслеживание истории использования документа, быстрый и удобный поиск.

4. Матрица ответственности

Для эффективного управления процессом обеспечения информационной безопасности в Товариществе применяется матрица ответственности за процессы и подпроцессы (отдельные элементы процесса).

Матрица ответственности устанавливает степень ответственности каждого участника процесса за выполнение отдельных этапов и задач. При составлении матрицы ответственности была использована методика RACI.

Методика RACI является удобным и наглядным средством планирования ответственности участников процесса при выполнении задач на каждом из этапов процесса.

Термин RACI является аббревиатурой:

- **Ответственный** (Accountable) – полностью отвечает за исполнение задачи, вправе принимать решения по способу реализации. В качестве ответственного за задачу может назначаться только один человек.
- **Исполнитель** (Responsible) – исполняет задачу, не несет ответственность за выбор способа её решения, но отвечает за качество и сроки реализации. У каждой задачи должен быть хотя бы один исполнитель.
- **Консультант** (Consult before doing) – оказывает консультации в ходе решения задач, контролирует качество реализации.
- **Наблюдатель** (Inform after doing) – может оказывать консультации в ходе решения задач процесса, не несет ответственности.

Этапы и задачи / Исполнители	Заместитель Генерального директора по технической политике и информационным технологиям	Служба контроля	Юридическая служба	Руководитель СИТ	Главный менеджер СИТ (администратор ЛВС)	Главный менеджер СИТ (администратор СЭД и прикладных информационных систем)	Главный менеджер СИТ (администратор серверов ИС 1С ERP)	Все работники Товарищества
Процесс управления информационной безопасностью	**О*К**	**К**	**Н**					
Подпроцесс №1: Административно-правовые и организационные меры				**ОИ**	**И**	**И**	**И**	**И**
Подпроцесс №2: Меры физической безопасности				**ОИ**	**И**	**И**	**И**	**И**
Подпроцесс №3: Программно-технические меры				**ОИ**	**И**	**И**	**И**	**И**

О* - ответственный за процесс;
К - консультант;
Н - наблюдатель;
О - ответственный за подпроцесс;
И - исполнитель.

5. Обеспечение работы процесса

5.1. Описание процесса

Политика управления информационной безопасностью является отдельным процессом и обязательной частью общей системы управления Товарищества.

Товарищество уделяет особое внимание вопросам обеспечения информационной безопасности, постоянно совершенствует систему

управления информационной безопасности, применяемые средства и способы защиты от угроз информационной безопасности, а также обеспечивает непрерывное обучение работников Товарищества для поддержания компетенции в области защиты информации на высоком уровне.

Политика информационной безопасности охватывает все информационные системы и документы, владельцем и пользователем которых является Товарищество. Обеспечение информационной безопасности является необходимым условием для успешного осуществления деятельности Товарищества. Информация является одним из важнейших активов Товарищества.

В основе Политики информационной безопасности Товарищества лежит риск-ориентированный подход, направленный на снижение вероятности реализации событий информационной безопасности.

Обеспечение информационной безопасности необходимо для снижения рисков и экономических потерь, связанных со всевозможными угрозами имеющимся информационным ресурсам Товарищества. С этой целью необходимо поддерживать главные свойства информации, а именно:

1) доступность - свойство, характеризующееся способностью своевременного беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия;
2) конфиденциальность - свойство, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней;
3) целостность - свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Основными объектами обеспечения информационной безопасности в Товариществе признаются следующие элементы:

1) информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством и внутренними нормативными документами Товарищества к коммерческой, служебной или иной охраняемой законом тайне;
2) средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети, системы), на которых производится обработка, передача и хранение защищаемой информации;
3) программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное ПО)

автоматизированных систем Товарищества, с помощью которых производится обработка защищаемой информации;

4) процессы Товарищества, связанные с управлением и использованием информационных ресурсов;
5) помещения, в которых расположены средства обработки защищаемой информации;
6) рабочие помещения и кабинеты работников, помещения Товарищества, предназначенные для ведения закрытых переговоров и совещаний;
7) работники Товарищества, имеющие доступ к защищаемой информации;
8) технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.

Подлежащая защите информация может:

размещаться на бумажных носителях;

существовать в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники, записываться и воспроизводиться с помощью технических средств);

передаваться по телефону, телефаксу, телексу и т.п. в виде электрических сигналов;

присутствовать в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров.

Построение системы обеспечения информационной безопасности Товарищества и ее функционирование должны осуществляется в соответствии со следующими принципами:

законность - любые действия, предпринимаемые для обеспечения, осуществляются на основе действующего законодательства, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты информации Товарищества;

ориентированность на бизнес - информационная безопасность рассматривается как процесс поддержки основной деятельности. Любые меры по обеспечению информационной безопасности не должны повлечь за собой серьёзных препятствий деятельности Товарищества;

непрерывность - применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты Товарищества должны осуществляться без прерывания или остановки текущих бизнес-процессов Товарищества;

комплексность - обеспечение безопасности информационных ресурсов в течении всего их жизненного цикла, на всех технологических этапах их

использования и во всех режимах функционирования;

обоснованность и экономическая целесообразность - используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать предъявляемым требованиям и нормам. Во всех случаях стоимость мер и систем информационной безопасности должна быть меньше размера возможного ущерба от любых видов риска;

приоритетность - категорирование (ранжирование) всех информационных ресурсов Товарищества по степени важности при оценке реальных, а также потенциальных угроз информационной безопасности;

необходимое знание и наименьший уровень привилегий - пользователь получает минимальный уровень привилегии и доступ только к тем данным, которые являются необходимыми для выполнения им деятельности в рамках своих полномочии;

эксплуатация технических средств и реализация мер информационной безопасности должны осуществляться профессионально подготовленными специалистами;

информированность и персональная ответственность - руководители всех уровней и исполнители должны быть осведомлены обо всех требованиях информационной безопасности и несут персональную ответственность за выполнение этих требований и соблюдение установленных мер информационной безопасности;

взаимодействие и координация - меры информационной безопасности осуществляются на основе взаимосвязи соответствующих структурных подразделений Товарищества, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями, профессиональными ассоциациями и сообществами, государственными органами, юридическими и физическими лицами;

подтверждаемость - важная документация и все записи - документы, подтверждающие исполнение требований по информационной безопасности и эффективность системы ее организации, должны создаваться и храниться с возможностью оперативного доступа и восстановления.

5.2. Описание этапов процесса

5.2.1. Административно-правовые и организационные меры

Административно-правовые и организационные меры включают (но не ограничены ими):

- контроль исполнения требований законодательства Республики Казахстан и внутренних документов Товарищества;
- разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих процедур информационной

безопасности;

- контроль соответствия бизнес-процессов Товарищества требованиям процедур информационной безопасности;
- информирование и обучение работников Товарищества работе с информационными системами и требованиям информационной безопасности;
- реагирование на каналы несанкционированной утечки информации, инциденты, связанные с этим, локализацию и минимизацию последствий;
- анализ новых рисков информационной безопасности;
- отслеживание и улучшение морально-делового климата в коллективе;
- определение действий при возникновении чрезвычайных ситуаций;
- проведение профилактических мер при приеме на работу и увольнении работников Товарищества.
- гарантия Товарищества о защите персональных данных работников, которая осуществляется путем применения комплекса мер, в том числе правовых, организационных и технических, в целях:
  1) реализации прав на неприкосновенность частной жизни, личную и семейную тайну;
  2) обеспечения их целостности и сохранности;
  3) соблюдения их конфиденциальности;
  4) реализации права на доступ к ним;
  5) предотвращения незаконного их сбора и обработки.

5.2.1.1. Оповещение об инцидентах информационной безопасности

Пользователи должны уметь распознавать возможные инциденты или попытки нарушения информационной безопасности и немедленно сообщать о них в Службу контроля и СИТ. Самостоятельное исследование инцидентов или попыток нарушения информационной безопасности запрещено и расценивается как атака на информационную безопасность Товарищества.

Признаки инцидентов информационной безопасности включают (но не ограничены ими):

- продолжительное по времени нахождение постороннего лица возле рабочей станции пользователя с явным намерением сфотографировать информацию с экрана монитора или скопировать информацию на съемный носитель;
- неожиданное блокирование учетных записей;
- продолжительное время входа/регистрации в ЛВС или информационной системе;
- появление в ЛВС неизвестных файлов;
- нарушение конфиденциальности;
- неожиданное искажение данных, появление в ЛВС или

информационных системах неверных или неполных данных;
- нештатное поведение, либо отказ ЛВС, отдельных ее сегментов или сервисов;
- нештатное поведение, либо отказ информационной системы.

Руководитель СИТ, как владелец риска нарушений информационной безопасности, после идентификации риска и определения степени его воздействия, обязан в суточный срок представить в Службу контроля следующую отчетность по управлению ключевыми рисками: Отчет о произошедших инцидентах за период (форма №1) и Отчет об изменении состояния ключевых рисков за период (форма №2).

Кроме этого, руководитель СИТ подготавливает пресс-релиз о произошедшем инциденте для публикации на закладке «Домашняя страница»-«Извещения» СЭД Товарищества.

5.2.1.2. Защита авторских прав

Многие программы, фильмы, электронные книги, музыкальные и иные мультимедийные файлы являются субъектами авторского права. Копирование и распространение таких файлов может быть запрещено.

Копирование, распространение, воспроизведение и хранение в ЛВС и на Рабочих станциях программ и контента, защищенного авторским правом, разрешено только с письменного разрешения правообладателя, или в других случаях, когда это считается «правомерным использованием».

Если у пользователя есть какие-либо вопросы относительно применимости законодательства об авторских правах, они должны обратиться за разъяснениями в Юридическую службу Товарищества.

Пользователи должны полагать, что все программы и прочие файлы защищены авторскими правами, если нет достоверной информации об обратном.

5.2.2. Меры физической безопасности

Меры физической безопасности включают (но не ограничены ими):
- организацию пропускного и внутри объектового режимов;
- построение периметра безопасности защищаемых объектов;
- организацию круглосуточной охраны охраняемых объектов, в том числе с использованием технических средств безопасности;
- организацию противопожарной безопасности охраняемых объектов;
- контроль доступа работников Товарищества в помещения ограниченного доступа.

5.2.2.1. Помещения ограниченного доступа

К помещениям ограниченного доступа в Товариществе относятся кроссовые и серверные помещения, архив, а также студии, залы совещаний и комнаты переговоров.

В кроссовые и серверные помещения доступ имеют:

- сотрудники СИТ для исполнения работ по обслуживанию и эксплуатации коммуникационного и серверного оборудования.

В архив доступ имеют:

- руководители Товарищества;
- сотрудники отдела архивирования;
- администратор СЭА.

В студии, залы совещаний и комнаты переговоров доступ имеют:

- руководители Товарищества и руководители структурных подразделений Товарищества;
- работники, приглашенные на совещания руководством Товарищества;
- пригашенные на переговоры, встречи, обсуждения, подписание контрактов контрагенты (по предварительному разрешению руководства Товарищества);
- представители компаний, проводящие тематические презентации (по предварительному разрешению руководства Товарищества);
- сотрудники СИТ для исполнения работ по обслуживанию и эксплуатации проекционного оборудования, оборудования видеоконференцсвязи, аудио-оборудования, оборудования синхронного перевода.

Посетители помещений ограниченного доступа должны быть проинструктированы о причинах ограничений, относящихся к помещению и предостережениях, которые должны быть выполнены.

Кроссовые и серверные помещения должны отвечать следующим требованиям:

- помещения должны постоянно находиться под охраной, полностью исключив при этом возможность бесконтрольного проникновения посторонних лиц;
- наличие системы видеонаблюдения и регистрации событий. Должна быть обеспечена возможность просмотра событий как в режиме online, так и любого архивного фрагмента. Длина архива должна составлять не менее 30 календарных дней;
- наличие стационарного телефона;
- наличие системы автоматического газового пожаротушения;
- наличие системы речевого оповещения о пожаре;
- наличие системы кондиционирования и охлаждения воздуха типа «зима-лето»;
- наличие энергонезависимой системы с вводным автоматическим выключателем и автоматическими выключателями на каждую розеточную группу;
- наличие специальной системы теплоотвода и дренажа;
- наличие рабочего места администратора ЛВС, оборудованное

необходимым комплектом мебели и компьютерной техники;

- доступ возможен только с помощью блокировки, карты доступа, ключа или других средств безопасности, выдаваемых лицом, ответственным за помещение.

Запрещается проведение уборки кроссовых и серверных помещений работниками клиннинговых служб без предварительного инструктажа и обязательного присутствия ответственного сотрудника СИТ.

Порядок доступа в кроссовые и серверные помещения, регистрация выдачи ключей, цели посещения и видов произведенных работ регламентируются отдельным внутренним документом о предоставлении доступа к инфраструктурному оборудованию Товарищества.

Обеспечение нормального функционирования комплекса технических средств (проекторов, аудио-микшеров, усилителей, оборудования видеоконференцсвязи, микрофонов, стереофонических устройств воспроизведения звука) студий, залов совещаний и комнат переговоров возложено на СИТ.

Исходя из возможности перехвата речевой информации при проведении разговоров конфиденциального характера с помощью внедрения специальных электронных устройств, акустических, виброакустических и лазерных технических средств, транслирующих эту информацию за пределы контролируемой зоны, противодействие угрозам безопасности информационных ресурсов должно осуществляться всеми доступными средствами и методами.

Студии, залы совещаний и комнаты переговоров должны быть визуально проверены сотрудниками СИТ на предмет отсутствия в них (в стеновых панелях, фальш-потолках и фальш-полах, мебели, технических средствах, размещенных в этих помещениях) закладных устройств, технических средств передачи данных, а также различных электрических и прочих цепей, не относящихся к линиям и средствам жизнеобеспечения здания.

В случае обнаружения, либо возникновения подозрения на использование технических средств, транслирующих защищаемую информацию за пределы контролируемой зоны, каждый сотрудник Товарищества обязан немедленно сообщить об этом в Службу контроля.

В студиях, залах совещаний и комнатах переговоров запрещается использовать фото и видеосъемку, мобильные телефоны и диктофоны без разрешения руководства Товарищества.

Для демонстрации в студиях, залах совещаний и комнатах переговоров видео-материалов (фильмы, видео-ролики) необходимо предварительное согласование с сотрудниками СИТ следующих условий:

- формат видео-материалов;

- продолжительность (минут);
- режим воспроизведения;
- источник видео-материала;
- ответственный за воспроизведение пользователь.

Пользователям запрещается самостоятельно устанавливать аудио-видео проигрыватели, а также плагины и дополнения к ним.

В целях усиления контроля за информационными ресурсами Товарищества допускается привлечение специализированных подрядных организаций, предоставляющих следующие услуги:

- предоставление проектных решений, обеспечивающих звукоизоляцию помещений;
- предоставление специальных средств обнаружения закладных устройств;
- установка временных или постоянных постов радио-контроля;
- предоставление устройств перехвата акустических сигналов с линий связи;
- предоставление фильтров и диэлектрических вставок, как систем активной защиты в акустическом и другом диапазонах.

5.2.3. Программно-технические меры

Программно-технические меры включают (но не ограничены ими):

- использование лицензионного ПО и сертифицированных средств защиты информации;
- использование средств защиты периметра (Firewall, IPS и т.п.);
- применение комплексной антивирусной защиты;
- использование средств информационной безопасности, встроенных в информационные системы;
- обеспечение регулярного резервного копирования информации;
- контроль за правами и действиями пользователей, в первую очередь, привилегированных;
- применение средств криптографической защиты информации в порядке, установленном нормативными правовыми актами;
- обеспечение безотказной работы аппаратных средств;
- мониторинг состояния критичных элементов информационной системы.

5.2.3.1. Учетные записи пользователей и пароли к ним

Для доступа к информационным ресурсам Товарищества каждому пользователю присваивается уникальная (в рамках ЛВС Товарищества) учетная запись – персональный идентификатор (логин) и пароль.

Учетная запись создается сотрудником СИТ только после представления пользователем копий следующих документов:

- приказ о приеме на работу в Товарищество;

- документ, удостоверяющий личность.

При создании новой учетной записи или в случае, если пользователь забыл свой пароль, ему предоставляется временный пароль, который он должен сменить при первом входе в ЛВС Товарищества.

Пользователи обязаны хранить свои пароли в тайне и соблюдать правила по обеспечению сложностей паролей:

- минимальная длина пароля – 8 символов;
- пароль не должен представлять собой легко угадываемые последовательности;
- пароль не должен состоять из одних и тех же цифр или букв.

Необходимо регулярно (не реже 1 раза в 60 дней) менять пароль.

Пароль следует менять на новый, не совпадающий с пятью предыдущими, каждые 60 дней или тогда, когда есть признаки того, что пароль пользователя был раскрыт. В последнем случае пароль необходимо поменять немедленно, не позднее одного рабочего дня.

Запрещается передавать свой логин и пароль другим пользователям и входить в информационные системы под логином других пользователей или другим любым способом выдавать себя за другое лицо в информационных системах Товарищества, других информационных системах и в сети Интернет.

Нельзя хранить логины и пароли в записанном виде в легкодоступных местах.

Пользователь несет ответственность за все действия, совершенные от лица его учётной записи.

Запрещается настраивать автоматический ввод паролей при входе на рабочую станцию или в информационные системы Товарищества.

При увольнении работника и представления последним подписанного обходного листа в СИТ, сотрудниками СИТ выполняются следующие действия с учетной записью уволенного работника:

- почтовый ящик удаляется немедленно без архивации содержимого;
- учетная запись пользователя деактивируется немедленно, а информация локального профиля удаляется после деактивации через 90 дней.

5.2.3.2. Безопасность рабочих станций пользователей

Товарищество предоставляет работникам рабочие станции для выполнения ими своих должностных обязанностей.

Настройку рабочих станций и установку на них стандартного ПО производят сотрудники СИТ. В случае необходимости установки дополнительного ПО или оборудования, изменения стандартных настроек или ремонта рабочих станций пользователь обращается в СИТ. Самостоятельный ремонт, внесение изменений в конфигурацию рабочих

станций, установка или удаление оборудования пользователями запрещены.

Самостоятельная установка ПО или запуск программ, кроме установленных сотрудниками СИТ, запрещены.

Пользователям запрещено предоставлять другим лицам (кроме работников СИТ) доступ к своим рабочим станциям, если на это нет распоряжения непосредственного руководителя пользователя.

Пользователи должны блокировать свою рабочую станцию (комбинация клавиш на клавиатуре «Ctrl + Alt + Del») когда покидают свое рабочее место в течение рабочего дня и выключать ее по окончании рабочего дня.

При вводе пароля и при работе с конфиденциальной информацией, пользователи должны убедиться, что посторонние лица не могут подсмотреть информацию с экрана монитора или вводимый пароль.

Пользователи обязаны использовать экранные заставки, автоматически включающиеся через 5 минут бездействия, для выхода из которых требуется пароль.

5.2.3.3. Защита от вирусов и вредоносного ПО

Весь комплекс работ по антивирусной защите ЛВС Товарищества осуществляет СИТ.

Запрещается соединение сервера или рабочей станции пользователя к ЛВС Товарищества без защиты обновленным антивирусным программным обеспечением.

Подрядные организации, которым необходимо подключить свой персональный компьютер или рабочую станцию к ЛВС Товарищества, должны получить предварительное разрешение сотрудников СИТ.

На всех рабочих станциях Товарищества используется система с сетевым управлением, где обновления антивирусных баз данных производятся в автоматическом режиме. Если такой возможности нет, на каждую рабочую станцию сотрудниками СИТ устанавливается автономное антивирусное ПО с автоматическим обновлением антивирусных баз данных.

Пользователям запрещается удалять установленные на их рабочие станции антивирусные программы или останавливать их работу.

При обнаружении или подозрении на наличие вируса или вредоносной программы, пользователь должен немедленно прекратить работу на рабочей станции и сообщить об этом в СИТ.

Удаление вирусов и вредоносных программ обычно происходит автоматически. Пользователям запрещается пытаться избавиться от вирусов или вредоносных программ самостоятельно.

Если есть подозрение, что предполагаемый вирус или вредоносная программа начала повреждать/удалять ПО или информацию пользователя, необходимо немедленно выключить рабочую станцию и сообщить об этом в

СИТ.

Пользователям запрещается сохранять, исследовать, создавать, пытаться внедрить и/или распространять вредоносные или саморазмножающиеся коды в какой-либо форме внутри и за пределами Товарищества.

5.2.3.4. Политика «чистого стола»

Обеспечение Политики «чистого стола» возложено на самих пользователей.

Пользователи должны обеспечить защиту информации любого вида (печатные копии, диски, USB-флэш-накопители и т.д.) в соответствии с категорией ее конфиденциальности.

Неиспользуемые документы, съемные носители и компьютерные средства (в особенности, в нерабочее время) должны храниться в подходящем для этих целей шкафу, желательно запираемом на ключ, и (или) в каких-либо других приспособлениях, обеспечивающих надлежащую сохранность.

Входящая и исходящая корреспонденция, а также факсимильные аппараты, не должны находиться в общедоступных местах.

Неиспользуемая конфиденциальная информация должна находиться в сейфах, запираемых на ключ шкафах, в частности, когда в офисе никого нет.

Запрещается оставлять без присмотра конфиденциальные документы при печати, сканировании, копировании или отправке по факсу.

5.2.3.5. Физическая безопасность

За каждой рабочей станцией или комплектом компьютерного оборудования закрепляется ответственное лицо. Прием оборудования и/или его передача другому ответственному лицу осуществляется только после оформления соответствующих документов материально-ответственным за оборудование лицом.

При увольнении пользователь обязан подписать обходной лист в СИТ.

Работникам запрещено приносить и подключать к ЛВС Товарищества свои собственные компьютеры (ноутбуки, планшетные ПК), или иное оборудование.

Ноутбуки или другое компьютерное оборудование, а также оргтехнику можно выносить из помещений Товарищества только при наличии материального пропуска. Материальный пропуск на имущество должен содержать информацию о марке (производителе) оборудования, краткую техническую характеристику, серийный, а также инвентарный номера.

Во время нахождения в командировках, а также при перелетах и переездах, ноутбуки необходимо носить как ручную кладь в портфеле или в специальной сумке для ноутбуков. Сканирование специальными средствами в аэропортах и на вокзалах не оказывает вредного воздействия на

информацию в компьютерах и на съемных носителях.

Нельзя оставлять компьютерное оборудование на сильной жаре или сильном холоде.

5.2.3.6. Использование ЛВС

Для организации взаимодействия и работы с внутренними и внешними информационными ресурсами, все рабочие станции и информационные системы Товарищества подключены к ЛВС, администрирование которой осуществляет СИТ.

В целях временного хранения, оперативного обмена и совместной работы с файлами в Товариществе используется файловый сервер обмена.

Для обеспечения надежности, пользователи должны хранить всю необходимую для работы информацию на рабочих станциях и сменных носителях. СИТ не гарантирует сохранность данных на файловом сервере обмена.

Пользователям запрещено открывать сетевой доступ к папкам и дискам рабочих станций.

В случае необходимости создания сетевого ресурса следует подать заявку в СИТ.

У всех совместно используемых ресурсов должен быть владелец. Владельцем является руководитель подразделения, которому принадлежит сетевой ресурс.

Всем пользователям по умолчанию должно быть отказано в доступе к общему ресурсу, за исключением случаев, когда доступ явно разрешен.

Доступ к группам может быть разрешен лишь тогда, когда СИТ получит письменное согласие от владельцев директории.

Ежегодно должны проводиться проверки прав доступа с владельцами директорий.

На всех совместно используемых папках должен быть активизирован контрольный след.

Пользователям запрещено использование программ, осуществляющих сканирование внутренней и внешних сетей, прослушивание и анализ сетевого трафика.

5.2.3.7. Корпоративная электронная почта и ресурсы Интернет

Корпоративная электронная почта в Товариществе является средством коммуникации, распределения информации и управления процессами в производственных целях: повышения эффективности труда работников Товарищества и экономии ее ресурсов.

Товарищество имеет единую защищенную точку выхода в сеть Интернет. Системы информационной безопасности контролируют доступ в Интернет из внутренней ЛВС Товарищества с целью обеспечения защиты от атак из сети Интернет, учета и оптимизации потребления трафика и

использования каналов связи, а также предотвращения выхода пользователей на вредоносные и опасные ресурсы Интернета.

Запрещается организация пользователями дополнительных подключений к Интернету из внутренней ЛВС Товарищества или другие попытки обхода системы контроля интернет-трафика.

При работе в сети Интернет пользователям, за исключением случаев служебной необходимости, запрещается:

- скачивать, сохранять и распространять, просматривать и прослушивать в режиме реального времени большие объемы данных (видео, музыка, изображения);
- скачивать и запускать программы;
- открывать и просматривать, а также сохранять и распространять информацию развлекательного, религиозного, клеветнического, дискриминационного, экстремистского, расистского, непристойного и криминального характера;
- посещать сайты, содержание которых не относится к должностным обязанностям работника;
- играть в различные игры и посещать интернет-казино и тотализаторы;
- использовать программы для зарабатывания денег в сети Интернет.

Наличие технической возможности посещения какого-либо определенного сайта не означает, что пользователям разрешено заходить на этот сайт.

Каждый работник Товарищества получает от СИТ корпоративный почтовый адрес вида фамилия_и@kamkor.org (где «фамилия» - фамилия пользователя на латинице, «и» - первая буква имени пользователя на латинице) в домене Товарищества. Адрес корпоративной электронной почты выдается сотрудником СИТ при начальной регистрации пользователя в домене Товарищества.

Размер почтового ящика пользователя ограничен 2 Гигабайтами.

Корпоративная электронная почта в Товариществе предназначена исключительно для использования в служебных целях.

При использовании корпоративной электронной почты и посещении ресурсов Интернета, пользователи могут явно (путем указания места работы и должности) или неявно (например, через адрес электронной почты или при выходе в Интернет из внутренней ЛВС Товарищества) ассоциироваться с Товариществом, поэтому, пользуясь этими средствами, они обязаны поддерживать имидж Товарищества путем выполнения следующих требований:

- осознанно создавать и поддерживать имидж Товарищества;
- относится к написанию электронного сообщения с такой же внимательностью и серьезностью, как и к разработке любого

документа Товарищества;

- в случае высказывания своего мнения в сообщениях корпоративной электронной почты или в сети Интернет, пользователи должны четко указывать, что высказываемые ими мнения являются их личными мнениями, которые могут не совпадать с мнением Товарищества.

Запрещается:

- использование корпоративной электронной почты для личной и иной переписки, не связанной с выполнением пользователями их должностных обязанностей;
- открывать вложения или ссылки в сообщениях электронной почты из непроверенных источников;
- использование корпоративной электронной почты для осуществления политической деятельности или благотворительной деятельности, не финансируемой Товариществом;
- открывать или запускать программы, полученные по электронной почте;
- пересылать конфиденциальные данные без применения средств шифрования;
- пересылать сообщения, содержащие вложения, размер которых превышает 30 Мегабайт;
- использование учетных записей других работников или отправка сообщений от чужого имени;
- пересылать «письма счастья», содержащие просьбу о пересылке другим адресатам.

Доступ к корпоративной электронной почте и сети Интернет с принадлежащих Товариществу рабочих станций за пределами ЛВС Товарищества должен осуществляться с соблюдением таких же правил, которые действуют при использовании электронной почты и Интернета во внутренней ЛВС Товарищества.

Работники не должны давать доступ к корпоративной электронной почте и информационным системам Товарищества членам своих семей или другим лицам, не являющимся работниками Товарищества.

Все почтовые сообщения, переданные или принятые с использованием корпоративной электронной почты Товарищества, принадлежат Товариществу и являются неотъемлемой частью ее производственного процесса.

5.2.3.8. Средства шифрования

В случаях производственной необходимости обмена защищаемой информацией через корпоративную электронную почту, информационные системы или сменные носители, передаваемая информация может быть зашифрована с помощью средств шифрования. Для этого Товарищество

должно располагать средствами шифрования информации, руководствоваться утвержденным регламентом и инструкциями по их применению.

Использование иных средств шифрования, кроме принятых в Товариществе, запрещено.

5.2.3.9. Сменные носители

В Товариществе разрешено использование как личных, так и служебных сменных носителей (USB-флэш-накопитель).

Риски информационной безопасности при их эксплуатации заключаются в следующем:

- угроза промышленного шпионажа;
- случайная утеря носителя, содержащего защищаемую информацию;
- искажение либо утеря (частичная или полная) информации при заражении носителя вирусом;
- выход носителя из строя.

Использование сменных носителей информации разрешено только в следующем порядке: при подключении к рабочей станции пользователь обязан произвести проверку содержимого носителя антивирусным ПО на предмет наличия вирусов и вредоносного ПО. Пользователям запрещается прерывать процесс сканирования сменного носителя антивирусным ПО.

Перед подключением сменного носителя к рабочей станции пользователь должен визуально осмотреть носитель на предмет отсутствия на нем трещин и физических повреждений, что может вызвать в дальнейшем выход из строя USB-порта рабочей станции.

При неудачных попытках подключения сменного носителя к рабочей станции пользователь должен обратиться в СИТ.

Традиционными методами защиты информации на сменных носителях должны являться:

- шифрованная файловая система EFS, позволяющая шифровать отдельные файлы и директории, и технология Bitlocker, шифрующая разделы сменных носителей;
- шифрование данных при помощи специальных утилит, которое удобнее для носителей, используемых для переноса информации, так как оно позволяет создавать шифрованные копии документов, не зависящие от операционных систем или файловой системы носителя;
- носители с поддержкой аппаратного шифрования, где для начала работы достаточно ввести PIN-код и подсоединить накопитель к USB-порту.

Помимо предотвращения возможности несанкционированного доступа к информации вследствие утери или хищения носителя, стоит также уделять

особое внимание сохранению ее доступности, что может быть реализовано комплексом организационных мер:

- пользователям запрещается хранить уникальную информацию на сменных носителях;
- для сменных носителей, обеспечивающих длительное хранение информации без постоянного доступа к ней (например, архивы и резервные копии), должны быть созданы условия хранения, обеспечивающие максимальную физическую сохранность с учетом их специфики;
- при длительном хранении информации необходимо регулярно проверять исправность сменных носителей и немедленно заменять их в случае выявления проблем. Создание дополнительных копий способствует уменьшению рисков потери защищаемой информации.

Пользователям необходимо соблюдать меры информационной безопасности при утилизации сменных носителей с защищаемой информацией. Сменные носители должны уничтожатся физически (чип памяти подлежит разрушению).

В случае использования сменных носителей для передачи персональных данных работников, для их уничтожения необходимо обратиться в СИТ, где будет произведено уничтожение носителя в присутствии пользователя, и при необходимости процесс уничтожения будет записан на видео.

5.2.3.10. Защита от атак методом социальной инженерии

Социальная инженерия – это обман или введение пользователей в заблуждение с целью выполнения пользователями желательных для злоумышленника действий или получения от пользователей информации или услуги. Для того, чтобы не стать жертвами социальной инженерии, необходимо принимать следующие меры:

- знать с кем вы говорите. Если вы не знаете звонящего лично или подозреваете, что звонящий не убедителен, выясните номер звонящего, и до того, как ему перезвонить, проверьте его легитимность;
- атаки методом социальной инженерии могут проводиться через электронную почту, веб-сайты и системы мгновенных сообщений. Имя и адрес, указанные в сообщении электронной почты, могут быть подделаны. Не отправляйте внутреннюю или иную другую конфиденциальную информацию на электронные адреса, которые вы не знаете или же не можете проверить;
- необходимо убедитесь в том, что запрашиваемая звонящим лицом информация, требуется ему для производственных нужд. Никогда не предоставляйте внутреннюю информацию, пока не установите, что она необходима звонящему лицу;

- запрещено открывать ссылки, файлы и вложения, полученные из неизвестных или непроверенных источников;
- в случае обнаружения или подозрения на атаку методом социальной инженерии необходимо срочно сообщить об инциденте в Службу контроля и СИТ.

5.2.3.11. Система электронного документооборота

Использование информационных технологий в управлении Товариществом, функционирование СЭД, позволяющее эффективно организовать процесс документационного обеспечения управления дают большие преимущества в работе, но и влекут за собой специфические проблемы. Одна из них – необходимость управления информационной безопасностью в СЭД и обеспечение защиты электронных документов, хранящихся в системе.

Администрирование СЭД Товарищества возложено на СИТ, а обеспечение информационной безопасности СЭД – на СИТ и всех работников Товарищества.

При обеспечении информационной безопасности в СЭД, необходим комплексный подход, который подразумевает защиту на всех уровнях:

Обеспечение сохранности документов

В большинстве случаев электронные документы, создаваемые сотрудниками, располагаются на локальных жестких дисках их компьютеров или на файловых серверах. Кроме того, что это неудобно, неэффективно с точки зрения взаимодействия сотрудников Товарищества, не обеспечивает разграничения прав доступа к документам, это также приводит к потерям документов, невозможности централизованного резервного копирования.

Документы в СЭД должны располагаться в Централизованном хранилище, в качестве которого выступает база данных под управлением SQL-сервера. Это обеспечивает безопасное хранение: документ не может быть утерян или уничтожен, так как среда хранения документов полностью контролируется СЭД, обеспечивается регулярное централизованное резервное копирование базы данных, доступ к данным ограничен только клиентским приложением СЭД в соответствии с установленными правами доступа. Ограничение доступа к данным СЭД только посредством клиентского приложения и API (объектной модели) является одним из важнейших требований к СЭД.

Обеспечение безопасного доступа к электронным документам

Любой пользователь в СЭД должен работает под своим именем и паролем. При этом поддерживается возможность использования имени и пароля, с которым пользователь вошел в операционную систему Windows (так называемая Windows-аутентификация).

Это позволяет решить ряд проблем безопасного доступа в СЭД. В первую очередь, это надежность выбираемых пользователями паролей. Не секрет, что пользователи склонны назначать простые для запоминания (а значит, и для подбора) пароли. За счет же применения политик безопасности домена Windows пароли учетных записей домена будут стойкими к взлому.

Вторым существенным преимуществом Windows-аутентификации является возможность интеграции с аппаратными средствами авторизации (смарт-карты, биометрические устройства), позволяющей обеспечить максимальную защиту компьютера от его использования при отсутствии пользователя-владельца сеанса. С хранением документов в единой базе данных становится возможным полноценное разграничение доступа к документам.

В СЭД должен быть реализован механизм задания прав доступа на каждый документ.

Существует четыре типа прав: права отсутствуют, есть права на просмотр, права на изменение и полные права на документ.

Расширяет возможности ограничения доступа пользователей к документам СЭД шифрование документов. Доступны два типа шифрования: шифрование на основе паролей и шифрование на основе сертификатов; возможно их комбинированное использование.

Обеспечение подлинности документов

Полноценное обеспечение подлинности электронного документа может быть достигнуто при использовании ЭЦП.

Электронная подпись необходима прежде всего в тех случаях, когда документ может потребоваться в качестве доказательства при судебном разбирательстве, для предоставления отчетности в органы государственной власти, например, в налоговую службу, или для обмена документами между юридическими лицами.

В СЭД Товарищества должен быть предусмотрен механизм подписания электронных документов ЭЦП, основанный на технологии шифрования с ассиметричным ключом, то есть владелец «подписи» должен владеть «закрытым» ключом и не допускать его передачу другим лицам, а «открытый» ключ может распространяться публично для проверки подлинности подписи, полученной при помощи «закрытого» ключа.

Протоколирование действий пользователей

В случае возникновения ситуаций непредусмотренного изменения текста или карточки документа, его удаления, доступа к документу пользователей, не имеющих на то права, большую помощь оказывает история работы с документом.

Функция ведения этой истории является обязательной для СЭДО.

Программно-аппаратная защита

Наряду с организационными мерами по обеспечению информационной безопасности СЭД необходимо дополнительно использовать механизмы, обеспечивающие (но не ограничены ими):

- контроль целостности используемого ПО СЭД;
- регистрацию событий;
- криптографическую защиту;
- межсетевое экранирование;
- виртуальные частные сети;
- антивирусную защиту;
- аудит информационной безопасности.

Дисциплинированность пользователей

Основное проблемное место при организации защиты СЭД, это не технические средства, а лояльность пользователей. Как только документ попадает к пользователю, конфиденциальность этого документа по отношению к пользователю уже нарушена.

Техническими мерами, в принципе, невозможно предотвратить утечку документа через этого пользователя. Основные средства защиты здесь - это организационные меры по ограничению доступа к конфиденциальным документам и работы с самим пользователем, который должен понимать степень своей ответственности перед Товариществом.

Запрещается настраивать автоматический ввод паролей при входе в СЭД.

Запрещается передавать свой логин и пароль другим пользователям и входить в СЭД под логином других пользователей или другим любым способом выдавать себя за другое лицо в СЭД.

Запрещается создавать дублирующие пересылки одних и тех же документов по СЭД и корпоративной электронной почте.

Запрещается хранить копии документов СЭД на файловом сервере обмена.

5.2.3.12. Безопасность информационных систем

Прикладные информационные системы - программы, предназначенные для решения задач или класса задач, связанных с обработкой данных в определенной области деятельности.

Эксплуатируемые в Товариществе прикладные информационные системы, вне зависимости от назначения, архитектуры и разработки (сторонними организациями, собственными силами сотрудников СИТ) являются базами данных.

База данных - структурированный организованный набор данных, описывающих характеристики какой-либо физической или виртуальной системы.

Защита баз данных Товарищества на сегодняшний день является актуальной проблемой, так как способность засекречивать информацию дает возможность быть уверенным в том, что информация, содержащаяся в базе данных, будет использоваться только определенными людьми для определенных целей.

Обязательным условием защиты базы данных является абсолютное (монопольное) владение базой данных, что подразумевает ее расположение (хостинг) на собственных серверных платформах Товарищества.

Администрирование баз данных Товарищества возложено на СИТ, а обеспечение их информационной безопасности – на СИТ и работников, имеющих доступ к базам данных Товарищества.

При эксплуатации баз данных Товарищества основными способами информационной защиты должны являться:

- строгое соблюдение пользователями внутренних регламентирующих документов по информационной безопасности при эксплуатации баз данных;
- маскировка персональных данных и данных, представляющих защищаемую информацию Товарищества;
- защита на уровне доменных политик;
- защита на уровне политики учетных записей, паролей, прав и разрешений в самой базе данных;
- защита при помощи терминального доступа к серверу;
- изменение расширений файлов;
- модификация файлов;
- изменение версий баз данных;
- шифрование значений таблиц.

Сторонние разработчики и сотрудники СИТ, при проектировании, разработке, а также на всех стадиях эксплуатации баз данных должны руководствоваться следующими принципами информационной безопасности:

Аутентификация пользователя и установление его идентичности

Проверка подлинности пользователя базы данных должна осуществляется либо через Windows-аутентификацию, либо через определенный SQL-оператор: пользователь идентифицируется своим именем, а средством аутентификации служит пароль.

Управление доступом к базам данных

Управление доступом к базам данных должно базироваться на реализации следующего минимального набора действий:

- произвольное управление доступом: метод ограничения доступа к объектам, основанный на учете личности пользователя или групп, в которую пользователь входит. Эта технология обеспечивает владельцу

объекта (представления, сервера базы данных, процедуры, таблице) передачу по своему усмотрению привилегий другому лицу;

- обеспечение безопасности повторного использования объектов: лишение прав для входа в информационную систему всех пользователей, покинувших Товарищество;
- использование меток безопасности: метка безопасности состоит из двух частей (уровня секретности и списка категорий). Первая составляющая зависит от приложения и в стандартном варианте может выглядеть как спектр значений от «совершенно секретно» до «несекретно». Вторая составляющая позволяет описать предметную область, разделяя информацию по отсекам, что способствует лучшей защищенности. Механизм меток безопасности не отменяет, а дополняет произвольное управление доступом, пользователи по-прежнему могут оперировать с таблицами только в рамках своих привилегий, получать только часть данных.
- принудительное управление доступом: основано на сопоставлении меток безопасности пользователя и объекта. Для чтения информации объекта необходимо доминирование метки пользователя над меткой объекта. При выполнении операции записи информации в объект необходимо доминирование метки безопасности объекта над меткой пользователя. Этот способ управления доступом называется принудительным, так как не зависит от воли пользователей.

Поддержание целостности данных

Обеспечение целостности данных не менее важная задана, чем управление доступом. С точки зрения пользователей баз данных, основными средствами поддержания целостности данных являются ограничения и правила. Ограничения могут содержаться непосредственно в реляционной модели данных, а могут задаваться в процессе создания таблицы. Табличные ограничения могут относиться к группе столбцов, отдельным атрибутам.

Ссылочные ограничения отвечают за поддержание целостности связей между таблицами. Ограничения накладываются владельцем таблицы и влияют на результат последующих операций с данными. Правила позволяют выполнять заданные процедуры при определенных изменениях базы данных.

В отличие от ограничений, которые обеспечивают контроль относительно простых условий, правила позволяют проверять и поддерживать соотношения любой сложности между элементами в базе данных.

Протоколирование и аудит

Протоколирование и аудит состоят в следующем:

- обнаружение необычных и подозрительных действий пользователей и идентификация лиц, совершивших эти действия;

- оценка возможных последствий состоявшегося нарушения;
- оказание помощи;
- организация пассивной защиты информации от нелегальных действий пользователя.

Защита коммуникаций между клиентом и сервером

Проблема защиты коммуникаций между клиентом и сервером не является специфичной для баз данных. Для обеспечения защиты информации выделяется сервис безопасности, в функции которого должны входить аутентификация, шифрование и авторизация.

Однако главный источник угроз для баз данных лежит в самой их природе. Нередко нужную, но недоступную по статусу информацию, можно получить путем логического вывода. Например, используя операцию добавления, а не выбора (на которую прав нет), можно анализировать коды завершения SQL-операторов.

Для борьбы с подобными угрозами должен использоваться механизм размножения строк для баз данных, поддерживающий метки безопасности. Агрегирование - метод получения новой информации путем комбинирования данных, добытых легальным путем из различных таблиц базы данных.

Инструкции и положения по эксплуатации баз данных наряду с регламентирующими, информационно-справочными и обучающими материалами должны содержать способы и методы обеспечения информационной безопасности.

Все имущественные права на базы данных, созданные в Товариществе как служебные произведения, должны быть зарегистрированы в органах юстиции.

Доступ разработчиков к продуктивным базам данных информационных систем Товарищества осуществляется сотрудниками СИТ только после согласования следующих параметров:

- подробное описание планируемых видов работ (модернизация, оптимизация, обновление и т.д.) и их продолжительность;
- тип доступа к базе данных (RDP-сессия, VPN-соединение, подключение посредством клиента удаленного доступа и т.д.);
- фамилия и должность разработчика, получающего доступ к продуктивной базе данных;
- описание возможных нештатных ситуаций после проведения работ с продуктивной базой данных;
- категории пользователей, для которых будет невозможен доступ в информационную систему во время проведения работ с продуктивной базой данных.

Сотрудникам СИТ запрещается предоставлять бессрочные постоянные параметры авторизации для разработчиков путем настройки постоянного

(неконтролируемого) доступа к продуктивным базам данных информационных систем.

Политики информационной безопасности прикладных информационных систем, предоставляемых на бесплатной основе финансовыми организациями и государственными органами (банк-клиенты, системы отправки/получения отчетности государственным органам) регламентируются собственными внутренними документами самих владельцев информационных систем и обязательны к исполнению пользователями.

5.2.3.13. Резервное копирование информации

Резервное копирование - процесс создания копии данных на носителе (жёстком диске, системе хранения данных, сменном носителе и т. д.), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

В этих целях в Товариществе должны применяться оба из двух видов копирования: собственными средствами серверных операционных систем и средствами специального ПО (в том числе и для теневого копирования).

Средства резервного копирования информации должны отвечать следующим требованиям:

- надёжность хранения информации - обеспечивается применением отказоустойчивого оборудования систем хранения, дублированием информации и заменой утерянной копии другой в случае уничтожения одной из копий (в том числе как часть отказоустойчивости);
- многоплатформенность - полноценное функционирование системы резервного копирования в гетерогенной сети предполагает, что ее серверная часть будет работать в различных операционных средах и поддерживать клиенты на самых разных аппаратно-программных платформах;
- простота в эксплуатации - автоматизация (по возможности минимизировать участие человека: как пользователя, так и администратора ЛВС);
- быстрое внедрение - простая установка и настройка программ, быстрое обучение пользователей.

Ключевыми параметрами резервного копирования должны являться:

RPO - Recovery Point Objective;

RTO - Recovery Time Objective.

RPO определяет точку отката - момент времени в прошлом, на который будут восстановлены данные, а RTO - определяет время, необходимое для восстановления из резервной копии.

В зависимости от целей, размера информации и критичности параметров RPO и RTO возможно применение следующих видов резервного копирования:

Полное резервное копирование (Full backup)

Полное копирование обычно затрагивает всю систему и все файлы, и подразумевает создание полной копии всех данных. Полное резервное копирование незаменимо в случае, когда нужно подготовить резервную копию для быстрого восстановления системы «с нуля».

Дифференциальное резервное копирование (Differential backup)

При дифференциальном («разностном») резервном копировании каждый файл, который был изменен с момента последнего полного резервного копирования, копируется каждый раз заново. Дифференциальное копирование ускоряет процесс восстановления. Все копии файлов делаются в определенные моменты времени, что, например, важно при заражении вирусами.

Инкрементное резервное копирование (Incremental backup)

При добавочном («инкрементном») резервном копировании происходит копирование только тех файлов, которые были изменены с тех пор, как в последний раз выполнялось полное или добавочное резервное копирование. В отличие от дифференциального копирования, изменившиеся или новые файлы не замещают старые, а добавляются на носитель независимо.

Клонирование

Клонирование позволяет скопировать целый раздел или носитель (устройство) со всеми файлами и директориями в другой раздел или на другой носитель. Если раздел является загрузочным, то клонированный раздел тоже будет загрузочным.

Резервное копирование в виде образа

Образ - точная копия всего раздела или носителя (устройства), хранящаяся в одном файле.

Резервное копирование в режиме реального времени

Резервное копирование в режиме реального времени позволяет создавать копии файлов, директорий и томов, не прерывая работу, без перезагрузки компьютера.

Холодное резервирование

При холодном резервировании база данных выключена или закрыта для потребителей. Файлы данных не изменяются, и копия базы данных находится в согласованном состоянии при последующем включении.

Горячее резервирование

При горячем резервировании база данных включена и открыта для потребителей. Копия базы данных приводится в согласованное состояние

путём автоматического приложения к ней журналов резервирования по окончании копирования файлов данных.

Сотрудникам СИТ, осуществляющим работы по резервному копированию информации, запрещается использовать для резервного копирования нелицензионное ПО.

График и порядок резервного копирования, жизненный цикл копий, места и объекты хранения резервной информации, виды резервного копирования, контрольные действия, ответственные за резервное копирование сотрудники СИТ и их ответственность за полноту, и актуальность информации регламентируются отдельным внутренним документом - Положением о системе резервного копирования Товарищества.

5.2.3.14. Социальные сети и мультимедиа-контент

В Товариществе не рассматривают социальные сети, как средство труда, и приравнивают их к средству потенциально опасного распространения защищаемой информации. Поэтому доступ к ним заблокирован, равно как и ко всем интернет-площадкам, сайтам, которые позволяют зарегистрированным на них пользователям размещать информацию о себе и коммуницировать между собой, устанавливая социальные связи.

Мультимедиа-контент не связан с выполнением пользователями их должностных обязанностей и потому должен быть заблокирован на всех рабочих станциях ЛВС Товарищества.

6. Результативность процесса

6.1. Критерии результативности процесса

Объективным критерием результативности процесса является обеспечение бесперебойного функционирования всего парка персональных компьютеров, серверного оборудования и корпоративной локально-вычислительной сети Товарищества в соответствии с показателями результативности процесса управления инфраструктурой (ИСМ КП 16 «Управление информационной безопасностью»), а также снижение вероятности реализации рисков информационной безопасности до приемлемого уровня в соответствии с утвержденными Правилами идентификации и оценки рисков Товарищества (Ссылка №3).

6.2. Мониторинг и анализ процесса

Процесс управления информационной безопасностью никогда не бывает законченным. В целях обеспечения достаточно надежной системы информационной безопасности, необходима постоянная переоценка ее параметров, адаптация для отражения новых опасностей, исходящих из внешней и внутренней среды. Не должно существовать каких-либо препятствий при внесении изменений в стандарты или процедуры по мере возникновения такой необходимости. В этой связи, определяются следующие

этапы цикла управления информационной безопасностью:

планирование (разработка) - анализ рисков, определение целей, задач, процессов, процедур, программно-аппаратных средств, относящихся к управлению рисками и совершенствованию информационной безопасности для получения результатов в соответствии с общей стратегией и целями Товарищества;

реализация (внедрение и эксплуатация) - внедрение и эксплуатация механизмов контроля, процессов, процедур, программно-аппаратных средств;

проверка (мониторинг и анализ) - измерение характеристик исполнения процессов в соответствии с процедурой, целями и практическим опытом, анализ изменения внешних и внутренних факторов, влияющих на защищенность информационных ресурсов, предоставления отчетов руководству для анализа;

корректировка (сопровождение и совершенствование) – принятие корректирующих и превентивных мер, основанных на результатах внутренних и внешних проверок состояния информационной безопасности, требований со стороны руководства, иных факторов, в целях обеспечения непрерывного совершенствования системы информационной безопасности.

6.3. Улучшение процесса

В Товариществе должны быть внедрены соответствующие процессы для обеспечения соблюдения требований нормативных правовых актов, соблюдения прав интеллектуальной собственности, защиты охраняемой законом персональной информации, соблюдения ограничений по использованию криптографических средств.

Все требования и положения международного стандарта ISO/IEC 27001 (Ссылка №2) являются обязательными для исполнения в области их применения, определяемой соответствующими документами.

При разработке и применении средств и методов информационной безопасности должны учитываться требования договорных обязательств и контрактов, заключенных Товариществом с третьими сторонами.

Доступ третьей стороны к информационным ресурсам Товарищества осуществляется только после анализа рисков, которые могут возникнуть при предоставлении такого доступа, и принятия адекватных защитных мер. В случае необходимости (в частности, при наличии требований нормативных правовых актов или международных стандартов), Товарищество проводит проверку контрагентов (поставщиков товаров и услуг) на соответствие определенным требованиям.

К государственным секретам и информации ограниченного распространения третьи стороны допускаются в порядке, установленном действующим законодательством.

На основании настоящей Политики разрабатывается ряд подчиненных внутренних нормативных документов, регламентирующих конкретные правила и методы обеспечения информационной безопасности, частные процедуры в области действия стандартов и т.п. Такие документы могут дополнять и расширять требования Политики, но не могут вступать с ней в противоречие.

7. Период действия, порядок внесения изменений и публикация

Настоящая политика вводится в действие приказом Генерального директора Товарищества. Политика признается утратившей силу на основании приказа Генерального директора Товарищества.

Изменения в Политику вносятся приказом Генерального директора Товарищества.

Инициаторами внесения изменений в Политику являются:

- Генеральный директор Товарищества;
- Заместители Генерального директора Товарищества;
- Служба контроля;
- Руководитель СИТ.

Актуализация настоящей Политики производится по требованию инициаторов, изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся информационной безопасности Товарищества, при происшествии и выявлении инцидента (инцидентов) по нарушению информационной безопасности, повлекших ущерб Товариществу, и имеет целью приведение в соответствие определенных Политикой защитных мер реальным условиям и текущим требованиям к защите информации.

Ответственным за актуализацию Политики является Руководитель СИТ.

Политика является общедоступным документом и публикуется на корпоративном сайте Товарищества www.kamkor.org в течение суток с момента издания приказа об утверждении Политики и вводе ее в действие.

8. Ответственность за соблюдение требований Политики

Все работники Товарищества несут персональную ответственность за нарушение и/или невыполнение требований Политики и процессов по защите информации и средств ее обработки, и обязаны незамедлительно сообщать обо всех выявленных нарушениях и инцидентах в Службу контроля и СИТ.

В случае нарушения установленных правил работы с информационными ресурсами работник Товарищества может быть ограничен в правах доступа к таким ресурсам, а также привлечен к ответственности в соответствии с действующим законодательством Республики Казахстан.

Должностные инструкции всех работников Товарищества должны содержать требования по обеспечению и соблюдению информационной безопасности.

9. Ссылки

Ссылка №1: СТ РК ИСО 9001-2016 Система менеджмента качества.

Ссылка №2: Международный стандарт ISO 27001:2013 «Информационные технологии - Методы обеспечения безопасности - Системы управления информационной безопасностью - Требования».

Ссылка №3: Правила идентификации и оценки рисков ТОО «Қамқор Менеджмент», утвержденные решением Наблюдательного совета ТОО «Қамқор Менеджмент» от 02.04.2012 года протокол №3.
