УТВЕРЖДАЮ
Директор
КГП на ПХВ «Областной центр крови»
КГУ «Управление здравоохранения акимата СКО»
Таукелов С.А._____

Полтика информационной безопасности КГП на ПХВ «Областной центр крови» КГУ «Управление здравоохранения акимата Северо-Казахстанской области»

г. Петропавловск, 2024 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 КГП на ПХВ «Областной центр крови» КГУ «Управление здравоохранения акимата Северо-Казахстанской области» (далее - Предприятие).

Информация является ценным активом Предприятия.

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

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

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

Доступ к информационным ресурсам Предприятия предоставляется только после ознакомления с настоящей Политикой и подписания работником Предприятия 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 Предприятия.

2. Область применения

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

Настоящая Политика является документом, доступным любому работнику Предприятия и пользователю его ресурсов, и представляет собой официально принятую руководством Предприятия систему обеспечения информационной безопасности, и управления ею на основе систематизированного изложения целей, процессов и процедур.

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

3. Термины и определения

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

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

Информационные ресурсы – документы и массивы документов в информационных системах.

Информационные системы – системы, предназначенные для хранения, поиска и обработки информации, и соответствующие организационные ресурсы, которые обеспечивают и распространяют информацию.

Локально-вычислительная сеть (ЛВС) – 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.

Подразделение IT специалистов – структурное подразделение, обособленное от других структурных подразделений, занимающихся вопросами создания, сопровождения и развития объектов информатизации, или определенное должностное лицо, ответственное за обеспечение информационной безопасности.

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

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 8, 8.1, 10, 11 и все последующие версии);
• комплект актуальных драйверов устройств;
• комплект актуальных обновлений для операционных систем Microsoft Windows;
• комплект офисных программ (Microsoft Office 2010, 2013, 2016, 2019, 2021 и все последующие версии);
• программу для просмотра электронных публикаций в формате PDF (Adobe Reader);
• антивирусное ПО с набором актуальных антивирусных баз.

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

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

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.

Социальная инженерия – это обман или введение пользователей в заблуждение с целью выполнения пользователями желательных для злоумышленника действий или получения от пользователей информации или услуги.

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.

ЭЦП – электронная цифровая подпись, реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи.

4. Обеспечение работы процесса

4.1. Общее

Управления информационной безопасностью является отдельным процессом и обязательной частью общей системы управления Предприятия.

Предприятие 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 Предприятия для поддержания компетенции в области защиты информации на высоком уровне.

Политика информационной безопасности охватывает все информационные системы и документы, владельцем и пользователем которых является Предприятие. Обеспечение информационной безопасности является необходимым условием для успешного осуществления деятельности Предприятия.

В основе информационной безопасности Предприятия 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 Предприятия. 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 на Предприятии признаются следующие элементы:

1) информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством и внутренними нормативными документами Предприятия 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 Предприятия, с помощью которых производится обработка защищаемой информации;

4) процессы Предприятия, связанные с управлением и использованием информационных ресурсов;

5) помещения, в которых расположены средства обработки защищаемой информации;

6) рабочие помещения и кабинеты работников Предприятия;

7) работники Предприятия, 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:

- размещается на бумажных носителях;
- существует в электронном виде (обрабатывается, передается и хранится средствами вычислительной техники, записывается и воспроизводится с помощью технических средств);

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

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

- законность – любые действия, предпринимаемые для обеспечения информационной безопасности, осуществляются на основе действующего законодательства;
- ориентированность на основную деятельность – информационная безопасность рассматривается как процесс поддержки основной деятельности Предприятия;
- непрерывность – применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты Предприятия осуществляются без прерывания или остановки текущих бизнес-процессов Предприятия;
- 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 реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и соответствуют предъявляемым требованиям и нормам;
- приоритетность – категорирование (ранжирование) всех информационных ресурсов Предприятия 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 полномочий;
- эксплуатация технических средств и реализация мер информационной безопасности осуществляются профессионально подготовленными специалистами;
- информированность и персональная ответственность – руководители всех уровней и исполнители 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 Предприятия, 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, создаются и хранятся с возможностью оперативного доступа и восстановления.

4.2. Описание этапов процесса

4.2.1. Административно-правовые и организационные меры

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

- контроль исполнения требований законодательства Республики Казахстан и внутренних документов Предприятия;
- разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих процедур информационной безопасности;
- контроль соответствия бизнес-процессов Предприятия требованиям процедур информационной безопасности;
- информирование и обучение работников Предприятия 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;
- определение действий при возникновении чрезвычайных ситуаций;
- проведение профилактических мер при приеме на работу и увольнении работников Предприятия;
- гарантия Предприятия о защите персональных данных работников и доноров, 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.

4.2.1.1. Оповещение об инцидентах информационной безопасности

Пользователи должны уметь распознавать возможные инциденты или попытки нарушения информационной безопасности и немедленно сообщать о них IT специалистам. Самостоятельное исследование инцидентов или попыток нарушения информационной безопасности запрещено и расценивается как атака на информационную безопасность Предприятия.

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.

4.2.1.2. 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 к юрисконсульту Предприятия.

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

4.2.2. 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 Предприятия в помещения ограниченного доступа.

К помещениям ограниченного доступа в ОЦК относятся серверное помещение и архив.

В серверное помещение доступ имеют:

- IT специалисты для исполнения работ по обслуживанию и эксплуатации коммуникационного и серверного оборудования.

В архив доступ имеют:

- руководитель Предприятия;
- сотрудники, представляющие архивную службу Предприятия.

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

Серверное помещение должно отвечать следующим требованиям:

- помещение должно 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 серверного помещения работниками Предприятия без предварительного инструктажа и обязательного присутствия ответственного сотрудника Предприятия.

Порядок доступа в серверное помещение, регистрация выдачи ключей, цели посещения и видов произведенных работ регламентируются отдельным внутренним документом (Журнал посещения серверного помещения).

Обеспечение нормального функционирования комплекса технических средств (проекторов, аудиомикшеров, усилителей, оборудования видеоконференцсвязи, микрофонов, стереофонических устройств воспроизведения звука) возложено на IT специалистов.

Для демонстрации видео-материалов (фильмы, видео-ролики) необходимо предварительное согласование с IT специалистами 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.

4.2.3. 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.

4.2.3.1. Учетные записи пользователей и пароли к ним

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

Учетная запись создается IT специалистом только после представления пользователем копий следующих документов:
- приказ о приеме на работу на Предприятие;
- 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 Предприятия.

Пользователи обязаны хранить свои пароли в тайне и соблюдать правила по обеспечению сложностей паролей:
- минимальная длина пароля – 5 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 Предприятия, 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 Предприятия.

При увольнении работника и представлении последним подписанного обходного листа IT специалистам, IT специалистами выполняются следующие действия с учетной записью уволенного работника:
- учетная запись пользователя деактивируется немедленно;
- информация локального профиля удаляется после деактивации через 90 дней.

4.2.3.2. Безопасность рабочих станций пользователей

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

Настройку рабочих станций и установку на них стандартного ПО производят IT специалисты. В случае необходимости установки дополнительного ПО или оборудования, изменения стандартных настроек или ремонта рабочих станций пользователь обращается к IT

специалистам. Самостоятельный ремонт, внесение изменений в конфигурацию рабочих станций, установка или удаление оборудования пользователями запрещены.

Самостоятельная установка ПО или запуск программ, кроме установленных IT специалистами, запрещены.

Пользователям запрещено предоставлять другим лицам (кроме IT специалистам) 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», либо Win + L) 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.

4.2.3.3. Защита от вирусов и вредоносного ПО

Весь комплекс работ по антивирусной защите ЛВС Предприятия осуществляют IT специалисты.

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

Подрядные организации, которым необходимо подключить свой персональный компьютер или рабочую станцию к ЛВС Предприятия, получают предварительное разрешение IT специалистов с согласия руководителя Предприятия.

На всех рабочих станциях Предприятия используется система с сетевым управлением, где обновления антивирусных баз данных производятся в автоматическом режиме. Если такой возможности нет, на каждую рабочую станцию IT специалистами 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 IT специалистам.

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

4.2.3.4. Политика «чистого стола»

Обеспечение Политики «чистого стола» возложено на самих пользователей.

Пользователи обеспечивают 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) хранятся 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 находится 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.

4.2.3.5. 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 у IT специалиста.

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

Ноутбуки или другие мобильные устройства, а также носители информации можно выносить из помещений Предприятия только при наличии записи в журнале выдачи мобильных устройств и носителей информации.

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.

Нельзя оставлять компьютерное оборудование на сильной жаре или сильном холоде.

4.2.3.6. Использование ЛВС

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

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

Совместно используемые ресурсы и общие папки создаются только на серверах Предприятия ITспециалистами.

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

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

4.2.3.7. Электронная почта и ресурсы Интернет

Электронная почта Предприятия является средством коммуникации, распределения информации и управления процессами в производственных целях: повышения эффективности труда работников Предприятия и экономии ее ресурсов.

Электронная почта Предприятия предназначена исключительно для использования в служебных целях.

При использовании 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 Предприятия) ассоциироваться с Предприятием, поэтому, пользуясь этими средствами, они обязаны поддерживать имидж Предприятия путем выполнения следующих требований:

- осознанно создавать и поддерживать имидж Предприятия;
- относится к написанию электронного сообщения с такой же внимательностью и серьезностью, как и к разработке любого документа Предприятия;
- в случае высказывания своего мнения в сообщениях электронной почты или в сети Интернет, пользователи должны четко указывать, что высказываемые ими мнения являются их личными мнениями, которые могут не совпадать с мнением Предприятия.

Запрещается:
- использование личной или иной почты, сервера которой расположены вне территории Республики Казахстан;
- использование электронной почты Предприятия 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 электронной почты для осуществления политической деятельности или благотворительной деятельности, не финансируемой Предприятием;
- 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 электронной почте и сети Интернет с принадлежащих Предприятию рабочих станций за пределами ЛВС Предприятия осуществляется с соблюдением таких же правил, которые действуют при использовании электронной почты и Интернета во внутренней ЛВС Предприятия.

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

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

Предприятие имеет единую защищенную точку выхода в сеть Интернет. Системы информационной безопасности контролируют доступ в Интернет из внутренней ЛВС Предприятия 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 Предприятия 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 заработка денег в сети Интернет.

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

4.2.3.8. Создание и использование ЭЦП

Электронная цифровая подпись (ЭЦП) – набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания, выданный

Национальным удостоверяющим центром Республики Казахстан, и подтверждающий легитимность электронного документа.

Предприятие в процессе своей деятельности использует ЭЦП. ЭЦП равнозначна собственноручной подписи подписывающего лица и влечет одинаковые юридические последствия при выполнении следующих условий:

1) удостоверена подлинность ЭЦП при помощи открытого ключа, имеющего регистрационное свидетельство;

2) лицо, подписавшее электронный документ, правомерно владеет закрытым ключом ЭЦП;

3) ЭЦП используется в соответствии со сведениями, указанными в регистрационном свидетельстве;

4) ЭЦП создана и регистрационное свидетельство выдано аккредитованным удостоверяющим центром Республики Казахстан или иностранным удостоверяющим центром, зарегистрированным в доверенной третьей стороне Республики Казахстан.

Закрытые ключи ЭЦП являются собственностью сотрудников Предприятия, владеющих ими на законных основаниях.

При необходимости сотрудник Предприятия может получить закрытые ключи ЭЦП для выполнения своих должностных обязанностей.

Создание ЭЦП в Предприятии возложено на IT специалистов. Перед созданием ЭЦП, IT специалист обязан ознакомить сотрудника с «Обязательством работника получаемого ЭЦП юридического лица».

После ознакомления сотрудник при согласии обязан собственноручно вписать в обязательство свои фамилию, имя, отчество, поставить роспись и дату создания ЭЦП. Сотрудник, для которого создается ЭЦП должен предоставить документ, удостоверяющий личность (паспорт или удостоверение личности), а также иметь при себе мобильный телефон с действующим номером, на котором он (сотрудник) зарегистрирован в базе мобильных граждан.

Закрытые ключи ЭЦП запрещено передавать другим сотрудникам и/или третьим лицам. Передача ЭЦП может за собой повлечь серьезный ущерб Предприятию, как материальный, так и репутационный.

Существуют следующие риски при передаче ЭЦП третьим лицам:

1. Совершение нелегитимных регистрационных действий;
2. Подлог официальных документов Предприятия;
3. Получение и передача третьим лицам конфиденциальной информации;
4. Подписать ошибочно либо некорректно составленных документов (например, налоговой отчетности).
5. Оформить фиктивные сделки;
6. Начислить премии или вывести со счетов Предприятия материальные средства.

При увольнении сотрудника IT специалист перед подписанием обходного листа обязан проверить наличие ЭЦП у данного сотрудника и при необходимости инициировать процесс отзыва ЭЦП.

4.2.3.9. Съёмные носители

На предприятии запрещается использование сменных носителей (USB-флэш-накопитель) на рабочих станциях.

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 осуществляется строго через IT специалиста в следующем порядке: при подключении к рабочей станции IT специалист обязан произвести проверку содержимого носителя антивирусным ПО на предмет наличия вирусов и

вредоносного ПО. IT специалистам запрещается прерывать процесс сканирования сменного носителя антивирусным ПО.

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

4.2.3.10. Защита от атак методом социальной инженерии

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 убедиться 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 IT специалистам.

4.2.3.11. Безопасность информационных систем

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

Эксплуатируемые на Предприятии прикладные информационные системы, вне зависимости от назначения, архитектуры и разработки (сторонними организациями, собственными силами IT специалистов) являются базами данных.

Защита баз данных Предприятия 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.

Администрирование баз данных Предприятия возложено на IT специалистов, а обеспечение их информационной безопасности – на IT специалистов и работников, имеющих доступ к базам данных Предприятия.

IT специалистам 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.

4.2.3.12. Резервное копирование информации

Для обеспечения процесса резервного копирования критически важных областей Предприятия используется NAS-сервер.

Средства резервного копирования информации отвечают 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);
- 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.

IT специалистам, 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 IT специалисты и их ответственность за полноту и актуальность информации регламентируются отдельным внутренним документом – Положением о системе резервного копирования Предприятия.

4.2.3.13. Социальные сети и мультимедиа-контент

На Предприятии 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. Исключение составляет рабочая станция, на которой ведутся социальные сети Предприятия ответственным работником для популяризации донорства.

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

5. Результативность процесса

5.1. Критерии результативности процесса

Объективным критерием результативности процесса является обеспечение бесперебойного функционирования всего парка персональных компьютеров, серверного оборудования и корпоративной локально- вычислительной сети Предприятия в соответствии с показателями результативности процесса управления инфраструктурой, а также снижение вероятности реализации рисков информационной безопасности до приемлемого.

5.2. 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.

Документированные стандартные операционные процедуры пересматриваются регулярно, не реже 1 (одного) раза в 3 (три) года, в случае необходимости - чаще. 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 Предприятия;
- 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.

5.3. Улучшение процесса

На Предприятии 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.

При разработке и применении средств и методов информационной безопасности учитываются требования договорных обязательств и контрактов, заключенных Предприятием с третьими сторонами.

Доступ третьей стороны к информационным ресурсам Предприятия 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), Предприятие 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.

6. Период действия, порядок внесения изменений и публикация

Настоящая политика вводится в действие после утверждения руководителем Предприятия.

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

Ответственными за актуализацию Политики являются IT специалисты.

Политика является общедоступным документом и публикуется на корпоративном сайте Предприятия http://ock.sko.kz.

7. Ответственность за соблюдение требований Политики

Все работники Предприятия 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 IT специалистам.

В случае нарушения установленных правил работы с информационными ресурсами работник Предприятия ограничивается в правах доступа к таким ресурсам, а также привлекается к ответственности в соответствии с действующим законодательством Республики Казахстан.

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