Стандарты и политики обеспечения информационной безопасности компании PepsiCo

Дата выпуска: апрель 2004 года

Последнее обновление: июль 2008 года

Содержание

1 Краткое описание

1.1 Введение

1.1.1 Цель

Настоящий документ содержит Стандарты и политики обеспечения информационной безопасности компании PepsiCo. Он предназначен для:

1. определения минимальных требований к защите информационных ресурсов компании PepsiCo;

2. передачи права собственности и ответственности за защиту информационных ресурсов компании PepsiCo;

3. принятия отдельными лицами взвешенных и соответствующих решений по защите информационных ресурсов компании PepsiCo.

1.1.2 Информационные ресурсы

Информация является существенным ресурсом, стимулирующим деятельность и длительную жизнеспособность компании PepsiCo. Настоящие Стандарты и политики обеспечения информационной безопасности применимы ко всем информационным ресурсам компании PepsiCo в электронном и физическом формате.

Процесс управления информационными рисками компании PepsiCo направлен на защиту конфиденциальности, целостности и доступности информации. Конфиденциальность относится к надлежащей защите информации с предоставлением доступа ограниченному количеству уполномоченных лиц. Целостность относится к информации, которая является полной, точной, контролируемой и воспроизводимой. Доступность относится к информации, функциям обработки данных и службам связи, которые готовы к использованию Сотрудниками компании PepsiCo в любом предполагаемом месте и времени.

1.1.3 Структура документа

Настоящий документ определяет важность информационной безопасности для компании PepsiCo и ее общую концепцию информационной безопасности. В нем представлена структура, основанная на иерархии принципов надлежащего управления рисками, включая Концепцию программы обеспечения информационной безопасности, политики и стандарты компании PepsiCo. Структура облегчает разработку, внедрение и обслуживание комплексных решений по обеспечению безопасности, соответствующих целям управления рисками компании PepsiCo.

Настоящий документ состоит из восьми разделов. В разделе описания определяются цель, должностные функции и обязанности сотрудников и область применения. Остальные семь разделов описывают политики обеспечения информационной безопасности. В каждом разделе политики указывается программное заявление, цели, обязанности сотрудников и стандарты.

Программные заявления являются краткими, и предполагается, что они будут актуальны и применимы в течение длительного периода времени (т.е. до тех пор, пока существенно не изменятся бизнес-назначение компании PepsiCo, цели безопасности или угрозы). В **стандартах** приводятся требования (т.е. приемлемый уровень обеспечения безопасности) и содержится большее количество измеряемых критериев для достижения общих целей, приведенных в политиках.

Процедуры не рассматриваются в настоящем документе, но они являются средствами выполнения стандарта (т.е. порядком действий для успешного выполнения требований стандарта) и могут меняться в зависимости от региона, подразделения или системной функции.

Настоящий документ не содержит процедуры

Все филиалы, структурные подразделения и дочерние предприятия компании PepsiCo несут ответственность за исполнение, обслуживание и применение процедур, необходимых для соблюдения Стандартов и политик обеспечения информационной безопасности компании PepsiCo.

1.2 Должностные функции и обязанности

Генеральный директор (CEO) компании PepsiCo является третьей и последней инстанцией по утверждению Стандартов и политик обеспечения информационной безопасности компании PepsiCo. CEO несет ответственность за пересмотр политик обеспечения информационной безопасности для обеспечения их соответствия корпоративному направлению деятельности.

Президент компании PepsiCo является второй инстанцией по утверждению Стандартов и политик обеспечения информационной безопасности компании PepsiCo. Подпись Президента официально устанавливает стандарты и политики обеспечения информационной безопасности для корпорации.

Руководитель по информационной безопасности (CISO) является первой инстанцией по утверждению Стандартов и политик обеспечения информационной безопасности компании PepsiCo. CISO несет ответственность за разработку, внедрение и обслуживание стандартов и политик обеспечения информационной безопасности.

Главный информационный директор (CIO) несет ответственность за предоставление руководства по технической выполнимости и экономической эффективности стандартов и политики обеспечения информационной безопасности, для соблюдения которых необходимо использование компьютерных систем. Кроме того, Группа компании PepsiCo по бизнес-решениям (PBSG) и иные должностные лица по информационным технологиям разрабатывают и придерживаются технического регламента, обеспечивающего выполнение стандартов и политик.

Менеджер по персоналу (CPO) несет ответственность за проверку воздействия политик и стандартов обеспечения информационной безопасности на Сотрудников. Отдел кадров несет ответственность за эффективное доведение политик до сведения сотрудников посредством обучения и информирования. Кроме того, начальник отдела кадров несет ответственность за консультирование CISO относительно соответствующих принудительных мер при несоблюдении политики и стандарта.

Главный внутренний аудитор компании PepsiCo несет ответственность за рассмотрение изменений, вносимых в стандарты и политики обеспечения информационной безопасности, а также за содействие при осуществлении аудита при необходимости. Кроме того, Отдел по управлению рисками и корпоративному аудиту несет ответственность за подтверждение соблюдения политики и стандартов.

Генеральный юрисконсульт несет ответственность за рассмотрение правовых аспектов внесения изменений в стандарты и политики обеспечения информационной безопасности, а при необходимости и за оказание CISO услуг по правовому сопровождению. Кроме того, генеральный юрисконсульт несет ответственность за обеспечение соответствия политик и стандартов законодательству и нормативным требованиям.

Владелец информации несет ответственность за определение требований к конфиденциальности, целостности и доступности для защиты его или ее коммерческих данных. Владельцы информации являются менеджерами организационных подразделений, которые несут основную ответственность за информационные ресурсы, связанные с их должностными полномочиями. Кроме того, Владельцы информации несут ответственность за определение процедур, поддерживающих стандарты и политики обеспечения информационной безопасности.

1.3 Область применения

Стандарты и политики обеспечения информационной безопасности компании PepsiCo применимы к Сотрудникам всех филиалов, дочерних предприятий, аффилированных компаний и совместных предприятий компании PepsiCo, при условии, что местные законы, правовые нормы и постановления правительства не заменяют собой данные политики и стандарты. **Сотрудниками** являются служащие, подрядчики, временные работники и работники, занятые неполный день, а также те, кто привлекается иными лицами для выполнения работы в помещениях компании PepsiCo или имеет доступ к информации, системам, компьютерам, сетям, телекоммуникациям и передачи сообщений и иным информационным службам компании PepsiCo.

1.4 Обязательства

Сотрудники подтверждают свои обязательства в отношении использования информационных систем и служб компании PepsiCo.

1. Обязательства Сотрудников включены в условия трудового договора или контактов, заключенных с компанией PepsiCo, Кодекс поведения и Стандарты и политики обеспечения информационной безопасности.
2. Сотрудники своей подписью и проставлением даты подтверждают, что они ознакомлены со своими обязательствами по обеспечению информационной безопасности.
3. Компания PepsiCo хранит подтверждающую документацию в соответствии с требованиями, приведенными в Политике управления документами компании PepsiCo.

1.5 Соблюдение и обеспечение выполнения обязательств

Сотрудники обязаны соблюдать Стандарты и политики обеспечения информационной безопасности компании PepsiCo.

1. Несоблюдение Сотрудником стандартов и политик может привести к принятию дисциплинарных мер вплоть до и включая увольнение сотрудников и расторжение договоров с подрядчиками, партнерами, консультантами или иными организациями.
   При нарушении действующего законодательства и норм также могут приниматься правовые меры.
2. CISO или уполномоченное лицо определяет серьезность случаев несоблюдения.
3. Уполномоченные лица Руководства филиала и Отдела кадров филиала (CPO) компании PepsiCo определяют последствия случаев несоблюдения.
4. Руководство филиала компании PepsiCo контролирует соблюдение требований своей организацией, определяет и принимает меры по устранению несоответствия и регистрирует соответствие существующим требованиям.
5. Руководство филиала компании PepsiCo хранит документацию по соблюдению требований в соответствии с требованиями, приведенными в Политике управления документами компании PepsiCo.

1.6 Работа с исключениями

Сотрудники выполняют действия, утвержденные CISO, при запросе исключений относительно соблюдения стандартов и политик обеспечения информационной безопасности.

1. CISO разрабатывает процедуру предоставления и оценки исключений относительно соблюдения существующих требований.
2. CISO рассматривает и утверждает исключения относительно соблюдения существующих требований и уведомляет Отдел по управлению рисками и корпоративному аудиту о предоставленных исключениях.

2 Допустимое использование

2.1 Правила допустимого использования

2.1.1 Программное заявление

Настоящие *Правила допустимого использования* определяют цели компании PepsiCo по созданию специальных стандартов по надлежащему коммерческому применению компьютерных систем и информационных ресурсов компании PepsiCo.

2.1.2 Цели

Информация, системы, службы и оборудование (например, настольные, портативные, карманные компьютеры, карманные персональные компьютеры (PDA), сети, Интернет, электронная почта, программное обеспечение, компьютерные приложения/системы, телефоны, пейджеры, голосовая почта и факсы) компании PepsiCo являются ресурсами компании и предназначены для использования в официальных и утвержденных деловых целях.

Использование информации, систем, служб и (или) оборудования, являющееся незаконным, оскорбительным и причиняющим беспокойство или ущерб компании PepsiCo или нарушающее Кодекс поведения компании PepsiCo, а также иные политики, стандарты и руководства компании PepsiCo, считается нарушением настоящей политики.

Компания PepsiCo сохраняет за собой право контролировать, регистрировать, разглашать и проверять свою информацию, системы, службы и оборудование. Специальные требования по допустимому использованию сети Интернет, электронной почты, телекоммуникаций, программного обеспечения, служб и оборудования приведены в стандартах по допустимому использованию.

2.1.3 Обязанности

Руководство филиала компании PepsiCo несет ответственность за доведение до сведения и рассмотрение в своих организационных подразделениях *Правил допустимого использования* и смежных стандартов. Руководство филиала компании PepsiCo также несет ответственность за определение, утверждение и выполнение процедур по обеспечению соблюдения политик и стандартов.

Сотрудники несут ответственность за изучение и соблюдение *Правил допустимого использования* и смежных стандартов.

2.2 Стандарт по допустимому использованию сети Интернет

Данный *Стандарт по допустимому использованию сети Интернет* основан на целях, приведенных в *Правилах допустимого использования*, и содержит специальные требования к правильному и надлежащему использованию интернет-ресурсов (например, интернет-соединения и браузеров).

2.2.1 Область применения

Настоящий стандарт относится к Сотрудникам, использующим интернет-ресурсы компании PepsiCo.

2.2.2 Принятие ответственности за соблюдение

Использование Сотрудником сети Интернет посредством компьютерных ресурсов компании PepsiCo является четко выраженным согласием соблюдать настоящий *Стандарт по допустимому использованию сети Интернет*.

2.2.3 Требования

A. Бизнес-применение

1. Сотрудники несут ответственность за работу сети Интернет, связанную с их учетными записями.
2. Интернет-ресурсы компании PepsiCo используются для деятельности, санкционированной компанией PepsiCo в соответствии с действующим законодательством и нормами.
3. Компания PepsiCo разрешает Сотрудникам периодически использовать свои интернет-ресурсы в личных целях, при условии, что данное использование не оказывает неблагоприятного влияния на работу компании PepsiCo.

B. Нецелевое использование (включая, среди прочего, следующее):

1. Интернет-ресурсы компании PepsiCo не должны использоваться для следующего:
   - Незаконная и ненадлежащая деятельность
   - Деятельность, влияющая на обычный ход работы компании
   - Деятельность, нарушающая Кодекс поведения или политики компании PepsiCo
   - Деятельность, препятствующая выполнению индивидуальной или иной работы Сотрудником
2. Интернет-ресурсы компании PepsiCo не должны использоваться для получения доступа, передачи, получения, распечатывания или хранения любого изображения, графика, документа, текста или иного материала, который может рассматриваться иными лицами как причиняющий беспокойство, унизительный, дискриминирующий или оскорбительный на основании их расовой, национальной принадлежности, цвета кожи, пола, сексуальной ориентации, возраста, ограниченных физических возможностей, статуса ветерана и религиозных или политических убеждений.

   Сотрудникам следует знать, что большое количество материалов может рассматриваться как причиняющее беспокойство, унизительное, дискриминирующее или оскорбительное.
3. Интернет-ресурсы компании PepsiCo не должны использоваться для преднамеренного отключения или перегрузки любой системы или сети или для обхода системы, предназначенной для защиты информации Сотрудника и (или) компании PepsiCo.
4. Интернет-ресурсы компании PepsiCo не должны использоваться для навязывания услуг, рекламирования или ведения коммерческой деятельности, не связанной с деятельностью компании PepsiCo.
5. Интернет-ресурсы компании PepsiCo не должны использоваться для разглашения информации, предназначенной для ограниченного пользования, без разрешения Руководства филиала компании PepsiCo.

   Информация, отправленная за пределы ресурса компании PepsiCo, может отслеживаться конкурентами компании PepsiCo. Более подробно о требованиях к классификации конфиденциальности смотрите в *Политике защиты ресурсов*.
6. Интернет-ресурсы компании PepsiCo не должны использоваться для мгновенной передачи сообщений без разрешения Руководства филиала компании PepsiCo.
7. Интернет-ресурсы компании PepsiCo не должны использоваться для преднамеренного совершения действий, которые расходуют компьютерные ресурсы или незаконно монополизируют ресурсы (например, отправка массовых рассылок или цепных писем, участие в чатах, игры и загрузка очень больших файлов).

   Интернет-ресурсы компании PepsiCo могут использоваться для участия в специальной деятельности (например, чаты, сетевые дневники (блоги) и форумы) только при выполнении действий, разрешенных компанией PepsiCo.
8. Интернет-ресурсы компании PepsiCo не должны использоваться для получения доступа к внешним сетевым службам электронной почты.

Процедуры обеспечения безопасности внешних сайтов могут не соответствовать требованиям *Политики защиты ресурсов* и могут вносить вирусы или иные вредоносные коды в компьютерную среду компании PepsiCo.

C. Интернет-браузер

1. Сотрудники должны использовать версии и конфигурации браузера, утвержденные компанией PepsiCo.
2. Сотрудники не должны изменять параметры безопасности браузера таким образом, чтобы они были менее ограничительными, чем конфигурации, утвержденные компанией PepsiCo.

D. Загружаемый материал

1. Сотрудники должны соблюдать действующее законодательство об авторском праве и лицензионные соглашения для материалов (например, программное обеспечение, файлы, документы, сообщения, графики, музыка или видео), загружаемых посредством интернет-ресурсов компании PepsiCo.
2. Сотрудники не должны загружать материал, требующий наличия лицензии, платы за регистрацию или не относящийся к деятельности компании PepsiCo, без разрешения Руководства филиала компании PepsiCo.
3. Сотрудники не должны выгружать, загружать, отправлять, получать, хранить или распечатывать следующие материалы без разрешения Руководства филиала компании PepsiCo:

   - Программное обеспечение (например, бесплатное программное обеспечение, условно-бесплатное программное обеспечение, коммерческое или общедоступное программное обеспечение)
   - Внешний материал от лиц или компаний, неизвестных Сотруднику
   - Информация компании PepsiCo или правительственная информация, предназначенная для ограниченного пользования (примеры приведены в Политике защиты ресурсов)

4. Сотрудники должны соблюдать процедуры, утвержденные компанией PepsiCo, по сканированию загружаемого материала и содержания на наличие вирусов и иных вредоносных кодов в соответствии с требованиями, приведенными в *Политике защиты ресурсов.*

E. Право на осуществление контроля

1. Компания PepsiCo сохраняет за собой право на осуществление контроля, регистрации, разглашения, аудита и удаления типа и содержимого деятельности Сотрудника с применением интернет-ресурсов компании PepsiCo без предварительного уведомления.

F. Ожидания неприкосновенности частной жизни

1. Сотрудники не должны рассчитывать на то, что их частная жизнь останется неприкосновенна при использовании интернет-ресурсов компании PepsiCo.
2. Компания PepsiCo сохраняет за собой право определять, какие действия можно совершать с информацией, полученной в результате деятельности Сотрудника (например, сообщения, рабочий продукт и резервные средства), осуществляемой с применением компьютерных (например, сеть Интернет) ресурсов компании PepsiCo.

   Действия могут включать, помимо прочего, разглашение характера и содержания деятельности сотрудникам правоохранительных органов или иным третьим лицам без предварительного уведомления Сотрудника. Деятельность Сотрудника может стать общедоступной.

G. Сообщение о неправильном использовании

1. Сотрудники должны сообщать о фактическом или предполагаемом неправильном использовании интернет-ресурсов компании PepsiCo и получении недопустимого содержимого в соответствии со *Стандартом по составлению отчетности о неправильном использовании.*
2. Сотрудники должны изменить сетевой пароль при обнаружении или возникновении подозрения о том, что кто-то еще знает данный пароль.

3. Сотрудники должны сразу же сообщить взломанные пароли в Центр технической поддержки компании PepsiCo или местный центр поддержки.

2.3 Стандарт по допустимому использованию электронной почты

Данный *Стандарт по допустимому использованию электронной почты* основан на целях, приведенных в *Правилах допустимого использования*, и содержит специальные требования к правильному и надлежащему использованию ресурсов электронной почты (например, программ и серверов электронной почты).

2.3.1 *Область применения*

Настоящий стандарт относится к Сотрудникам, использующим ресурсы электронной почты компании PepsiCo.

2.3.2 Принятие ответственности за соблюдение

Использование Сотрудником электронной почты посредством компьютерных ресурсов компании PepsiCo является четко выраженным согласием соблюдать настоящий *Стандарт по допустимому использованию электронной почты*.

2.3.3 Требования

A. *Бизнес-применение*

1. Сотрудники несут ответственность за работу электронной почты, связанную с их учетными записями.
2. Сотрудники должны защищать информацию для ограниченного и внутреннего пользования, доступ к которой обеспечивается и (или) которая хранится на ресурсах электронной почты, в соответствии с требованиями *Политики защиты ресурсов.*
3. Ресурсы электронной почты компании PepsiCo должны использоваться только для официально утвержденных целей компании PepsiCo.
4. При необходимости Руководство филиала компании PepsiCo уполномочивает ограниченное количество Сотрудников в качестве агентов относительно возможностей электронной почты иных Сотрудников (т.е. помощник по административным вопросам может читать или создавать электронные письма от лица руководства).

   Обмен учетными данными для проверки подлинности или паролями запрещен.
5. Компания PepsiCo может создавать учетные записи внешней (например, в сети Интернет) электронной почты, которые направляют входящий поток сообщений в «Список рассылки» или «Почту в базе данных» в системах передачи сообщений компании PepsiCo.
6. Компания PepsiCo разрешает Сотрудникам периодически использовать свои ресурсы электронной почты в личных целях, при условии, что данное использование не оказывает неблагоприятного влияния на работу компании PepsiCo.

B. *Нецелевое использование (включая, среди прочего, следующее):*

1. Сотрудники не должны идентифицироваться как иной Сотрудник, создавать ложные или вводящие в заблуждение заголовки сообщений электронной почты или оказывать несанкционированные услуги по передаче сообщений.
2. Ресурсы электронной почты компании PepsiCo не должны использоваться для следующего:

   - Незаконная и ненадлежащая деятельность
   - Деятельность, которая служит помехой обычному ходу работы■ Деятельность, нарушающая Кодекс поведения или политики компании PepsiCo
   - Деятельность, препятствующая выполнению индивидуальной или иной работы Сотрудником
3. Ресурсы электронной почты компании PepsiCo не должны использоваться для получения доступа, передачи, получения, распечатывания или хранения следующих видов материалов:

   - Приносящие беспокойство, унизительные, дискриминирующие или оскорбительные сообщения.
   - Незапрашиваемые сообщения лицам, не желающим их получать (например, «спамминг»).
   - Сообщения или изображения, имеющие порнографический или явный сексуальный характер.

- Рассылки в личных, политических или иных целях, не имеющие отношение к деятельности компании PepsiCo.
- Цепные письма, сообщения типа «шутка дня», сообщения, связанные со спортивными тотализаторами и азартными играми, или ложные предупреждения о возможном наличии вирусов и иные программы-мистификации.
- Сообщения, содержащие рекомендации любого юриста компании PepsiCo или стороннего юрисконсульта для любого иного лица, не являющегося уполномоченным получателем компании PepsiCo.
- Шутки, комментарии или изображения, содержащие оскорбительные выпады на национальной почве, расистские эпитеты или любые иные сообщения, которые могут оскорблять, порочить или компрометировать иных лиц на основании их расовой, национальной принадлежности, цвета кожи, пола, сексуальной ориентации, возраста, ограниченных физических возможностей, статуса ветерана, религиозных или политических убеждений или по иным причинам, неприятным для получателя.

Сотрудникам следует знать, что большое количество материалов может рассматриваться как приносящее беспокойство, унизительное, дискриминирующее или оскорбительное.

4. Ресурсы электронной почты компании PepsiCo не должны использоваться для преднамеренного отключения или перегрузки любой системы или сети или для обхода системы, предназначенной для защиты информации Сотрудника и (или) компании PepsiCo.

5. Ресурсы электронной почты компании PepsiCo не должны использоваться для навязывания услуг, рекламирования или ведения коммерческой деятельности, не связанной с деятельностью компании PepsiCo.

6. Ресурсы электронной почты компании PepsiCo не должны использоваться для разглашения информации, предназначенной для ограниченного пользования, без разрешения Руководства филиала компании PepsiCo.

   Информация, отправленная за пределы ресурса компании PepsiCo, может отслеживаться конкурентами компании PepsiCo. Более подробно о требованиях к классификации конфиденциальности смотрите в *Политике защиты ресурсов*.

7. Ресурсы электронной почты компании PepsiCo не должны использоваться для мгновенной передачи сообщений без разрешения Руководства филиала компании PepsiCo.

8. Ресурсы электронной почты компании PepsiCo не должны использоваться для преднамеренного совершения действий, которые расходуют компьютерные ресурсы или незаконно монополизируют ресурсы (например, отправка массовых рассылок или цепных писем, участие в чатах, подписка на списки электронных рассылок, не связанных с деятельностью компании PepsiCo, игры и загрузка очень больших файлов).

   Ресурсы электронной почты компании PepsiCo могут использоваться для участия в специальной деятельности (например, чаты, сетевые дневники (блоги) и форумы) только при выполнении действий, разрешенных компанией PepsiCo.

9. Ресурсы электронной почты компании PepsiCo не должны использоваться для ведения официального учета.

   Записи электронной почты, которые необходимо сохранять дольше 90 (девяноста) дней в нормативных, правовых финансовых или деловых целях, хранятся в соответствии с требованиями, приведенными в Политике управления документами компании PepsiCo.

C. Программное обеспечение электронной почты

1. Сотрудники должны использовать версии и конфигурации программного обеспечения электронной почты, утвержденные компанией PepsiCo.

2. Сотрудники не должны изменять параметры безопасности электронной почты таким образом, чтобы они были менее ограничительными, чем конфигурации, утвержденные компанией PepsiCo.

3. Сотрудники не должны использовать программное обеспечение или средства, автоматически переадресовывающие сообщения электронной почты, если только данное действие не разрешено Руководством филиала компании PepsiCo.

4. Сотрудники не должны использовать программное обеспечение или средства, подделывающие или скрывающие личность отправителя сообщения.

5. Сотрудники не должны разглашать иных получателей электронной почты при отправлении любой информации, кроме общедоступной, за пределами систем передачи сообщения компании PepsiCo в целях соблюдения правил хорошего тона.

   Сотрудники должны отдать предпочтение использованию слепой копии для иных получателей. Более подробно о требованиях к классификации конфиденциальности смотрите в *Политике защиты ресурсов*.

6. Системы обмена электронными сообщениями компании PepsiCo должны включать средства обеспечения безопасности (например, сканирование электронной почты на наличие вирусов) на границе между частной сетью компании PepsiCo и иными сетями, защищающие внутреннюю информацию компании PepsiCo и внешние системы.

   Системы обмена электронными сообщениями (например, мгновенные сообщения), которые не могут обеспечить необходимый уровень защиты, не должны пересекать границу.

D. Загружаемый материал

1. Сотрудники должны соблюдать действующее законодательство об авторском праве и лицензионные соглашения для материалов (например, программное обеспечение, файлы, графики, документы, сообщения, музыка или видео), загружаемых посредством ресурсов электронной почты компании PepsiCo.

2. Сотрудники не должны загружать материал, требующий наличия лицензии, платы за регистрацию или не относящийся к деятельности компании PepsiCo, без разрешения Руководства филиала компании PepsiCo.

3. Сотрудники не должны выгружать, загружать, отправлять, получать, хранить или распечатывать следующие материалы без разрешения Руководства филиала компании PepsiCo:

   - Программное обеспечение (например, бесплатное программное обеспечение, условно-бесплатное программное обеспечение, коммерческое или общедоступное программное обеспечение)
   - Внешний материал от лиц или компаний, неизвестных Сотруднику
   - Информация компании PepsiCo или правительственная информация, предназначенная для ограниченного пользования (примеры приведены в *Политике защиты ресурсов*)

4. Сотрудники должны соблюдать процедуры, утвержденные компанией PepsiCo, по сканированию содержания сообщений электронной почты и приложений на наличие вирусов и иных вредоносных кодов в соответствии с требованиями, приведенными в *Политике защиты ресурсов.*

E. Право на осуществление контроля

1. Компания PepsiCo сохраняет за собой право на осуществление контроля, регистрации, разглашения, аудита и удаления типа и содержимого деятельности Сотрудника с применением ресурсов электронной почты компании PepsiCo без предварительного уведомления.

F. Ожидания неприкосновенности частной жизни

1. Сотрудники не должны рассчитывать на то, что их частная жизнь останется неприкосновенной при использовании ресурсов электронной почты компании PepsiCo.

2. Компания PepsiCo сохраняет за собой право определять, какие действия могут совершаться с информацией, полученной в результате деятельности Сотрудника (например, сообщения, рабочий продукт и резервные средства), осуществляемой с применением компьютерных (например, электронная почта) ресурсов компании PepsiCo.

   Действия могут включать, помимо прочего, разглашение характера и содержания деятельности сотрудникам правоохранительных органов или иным третьим лицам без предварительного уведомления Сотрудника. Деятельность Сотрудника может стать общедоступной.

G. Емкость запоминающего устройства и срок хранения сообщений электронной почты

1. Сообщения и приложения электронной почты Сотрудника хранятся в соответствии с требованиями, приведенными в Политике управления документами компании PepsiCo.
2. Сообщения и приложения электронной почты компании PepsiCo (отправленные и полученные) не должны превышать предельные размеры файлов, установленные Руководством филиала.

Текущий предельный размер корпоративного файла для сообщений и приложений электронной почты составляет пять мегабайт (5 Мб).

H. Сообщение о неправильном использовании

1. Сотрудники должны сообщать о фактическом или предполагаемом неправильном использовании ресурсов электронной почты компании PepsiCo и получении недопустимого содержимого в соответствии со *Стандартом по составлению отчетности о неправильном использовании.*
2. Сотрудники должны изменить пароль электронной почты при обнаружении или возникновении подозрения о том, что кто-то еще знает данный пароль.
3. Сотрудники должны сразу же сообщить взломанные пароли в Центр технической поддержки компании PepsiCo или местный центр поддержки.

I. Право собственности на электронную почту

1. Право собственности на систему обмена электронными сообщениями, включающую оборудование и информацию, сообщения и приложения, созданные, отправленные, скопированные или доступные непосредственно или косвенно, принадлежит компании PepsiCo.

J. Защита информации для ограниченного или внутреннего пользования

1. Сотрудники должны включать следующую запись в сообщения электронной почты, содержащие информацию, предназначенную для ограниченного пользования, или при общении с третьими лицами (например, поставщик или консультант, участвующие в деятельности компании PepsiCo):

   «ДАННОЕ СООБЩЕНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ И ЕГО СОДЕРЖАНИЕ ПРЕДНАЗНАЧЕНЫ ТОЛЬКО ДЛЯ ПОЛЬЗОВАНИЯ АДРЕСУЕМЫМИ ПОЛУЧАТЕЛЯМИ И МОЖЕТ СОДЕРЖАТЬ ИНФОРМАЦИЮ, ЯВЛЯЮЩУЮСЯ СЛУЖЕБНОЙ, КОНФИДЕНЦИАЛЬНОЙ ИЛИ НЕ ПОДЛЕЖАЩЕЙ РАЗГЛАШЕНИЮ СОГЛАСНО ДЕЙСТВУЮЩЕМУ ЗАКОНОДАТЕЛЬСТВУ. ЕСЛИ ВЫ НЕ ЯВЛЯЕТЕСЬ НАЗНАЧЕННЫМ ПОЛУЧАТЕЛЕМ ИЛИ АГЕНТОМ, ОТВЕТСТВЕННЫМ ЗА ДОСТАВКУ ДАННОГО ЭЛЕКТРОННОГО СООБЩЕНИЯ НАЗНАЧЕННОМУ ПОЛУЧАТЕЛЮ, НАСТОЯЩИМ ВЫ УВЕДОМЛЯЕТЕСЬ О ТОМ, ЧТО ЛЮБОЕ ИСПОЛЬЗОВАНИЕ, РАСПРОСТРАНЕНИЕ, РАСПРЕДЕЛЕНИЕ ИЛИ КОПИРОВАНИЕ ДАННОГО СООБЩЕНИЯ СТРОГО ЗАПРЕЩЕНО И МОЖЕТ БЫТЬ НЕЗАКОННЫМ. ЕСЛИ ВЫ ПОЛУЧИЛИ ДАННОЕ СООБЩЕНИЕ ПО ОШИБКЕ, СРАЗУ ЖЕ СООБЩИТЕ ОБ ЭТОМ ОТПРАВИТЕЛЮ, ОТВЕТИВ НА ДАННОЕ ПИСЬМО ИЛИ ПО ТЕЛЕФОНУ, И УДАЛИТЕ ЭЛЕКТРОННОЕ ПИСЬМО, ОТПРАВЛЕННОЕ ПО ОШИБКЕ».

   При необходимости Сотрудники могут изменять текст для соответствия местному языку и нормативным требованиям.

K. Использование списков рассылки

1. Сотрудники должны ограничивать количество получателей информации, предназначенной для ограниченного пользования, по принципу служебной необходимости.
2. Компания PepsiCo должна внедрить процесс в рамках групп по вопросам коммуникации компании PepsiCo, который бы обеспечивал контроль качества и гарантию электронных писем, предназначенных широкой публики (например, более 100 Сотрудников).

2.4 Стандарт по допустимому использованию телекоммуникаций

Данный *Стандарт по допустимому использованию телекоммуникации* основан на целях, приведенных в *Правилах допустимого использования*, и содержит специальные требования к правильному и надлежащему использованию ресурсов телекоммуникаций (например, телефоны, сотовые телефоны, факсы и голосовая почта).

2.4.1 Область применения

Настоящий стандарт относится к Сотрудникам, использующим ресурсы телекоммуникаций компании PepsiCo.

2.4.2 Принятие ответственности за соблюдение

Использование Сотрудником ресурсов телекоммуникаций компании PepsiCo является четко выраженным согласием соблюдать настоящий *Стандарт по допустимому использованию телекоммуникации*.

2.4.3 Требования

A. Бизнес-применение

1. Сотрудники несут ответственность за работу, связанную с использованием ресурсов телекоммуникаций, предоставленных компанией PepsiCo.
2. Сотрудники должны защищать информацию для ограниченного и внутреннего пользования, доступ к которой предоставляется, которая обрабатывается и (или) хранится на ресурсов телекоммуникаций, в соответствии с требованиями *Политики защиты ресурсов*.
3. Ресурсы телекоммуникаций компании PepsiCo используются для деятельности, санкционированной компанией PepsiCo в соответствии с действующим законодательством и нормами.
4. Компания PepsiCo разрешает Сотрудникам периодически использовать свои ресурсы телекоммуникаций в личных целях, при условии, что данное использование не оказывает неблагоприятного влияния на работу компании PepsiCo.

B. Нецелевое использование (включая, среди прочего, следующее):

1. Ресурсы телекоммуникаций компании PepsiCo не должны использоваться для следующего:
   - Незаконная и ненадлежащая деятельность
   - Деятельность, влияющая на обычный ход работы компании
   - Деятельность, нарушающая Кодекс поведения или политики компании PepsiCo
   - Деятельность, препятствующая выполнению индивидуальной или иной работы Сотрудником
2. Ресурсы телекоммуникаций компании PepsiCo не должны использоваться для получения доступа, передачи, получения, распечатывания или хранения любого изображения, графика, документа, текста или иного материала, который может рассматриваться иными лицами как приносящий беспокойство, унизительный, дискриминирующий или оскорбительный на основании их расовой, национальной принадлежности, цвета кожи, пола, сексуальной ориентации, возраста, ограниченных физических возможностей, статуса ветерана и религиозных или политических убеждений.

   Сотрудникам следует знать, что большое количество материалов может рассматриваться как приносящее беспокойство, нарушающее, дискриминирующее или оскорбительное.
3. Ресурсы телекоммуникаций компании PepsiCo не должны использоваться для преднамеренного совершения действий, которые расходуют компьютерные ресурсы или незаконно монополизируют ресурсы (например, отправка массовых рассылок или цепных писем, участие в чатах, игры и загрузка очень больших файлов).

   Ресурсы телекоммуникаций компании PepsiCo могут использоваться для участия в специальной деятельности (например, чаты и форумы) только при выполнении действий, разрешенных компанией PepsiCo.

4. Ресурсы телекоммуникаций компании PepsiCo не должны использоваться для преднамеренного отключения или перегрузки любой системы или сети или для обхода системы, предназначенной для защиты информации Сотрудника и (или) компании PepsiCo.
5. Ресурсы телекоммуникаций компании PepsiCo не должны использоваться для навязывания услуг, рекламирования или ведения коммерческой деятельности, не связанной с деятельностью компании PepsiCo.
6. Ресурсы телекоммуникаций компании PepsiCo не должны использоваться для разглашения информации, предназначенной для ограниченного пользования, без разрешения Руководства филиала компании PepsiCo.

   Информация, отправленная за пределы ресурса компании PepsiCo, может отслеживаться конкурентами компании PepsiCo. Более подробно о требованиях к классификации конфиденциальности смотрите в *Политике защиты ресурсов.*
7. Ресурсы телекоммуникаций компании PepsiCo не должны использоваться для мгновенной передачи сообщений без разрешения Руководства филиала компании PepsiCo.

C. Телефонные ресурсы компании PepsiCo

1. Сотрудники объявляют об использовании громкоговорящей связи, микрофонов, громкоговорителей, магнитофонов, видеомагнитофонов и магнитофонов видео-конференц-связи и (или) аналогичного оборудования всем участникам вызова или конференции в целях соблюдения правил хорошего тона.
2. Сотрудники должны использовать междугородные и конференц-вызовы для деловых целей компании PepsiCo, как определено Руководством филиала компании PepsiCo.
3. Сотрудники должны принимать меры предосторожности при обсуждении конфиденциальной или производственной информации в местах, где данная информацию может быть услышана неуполномоченным третьим лицом.

D. Голосовая почта

1. Сотрудники должны использовать пароли голосовой почты, а не пароли системы по умолчанию.
2. Сотрудники не должны переадресовывать вызовы за пределы внутреннего телефонного ресурса компании PepsiCo.
3. Голосовая почта Сотрудника хранится в соответствии с требованиями, приведенными в Политике управления документами компании PepsiCo.

E. Факсы

1. Сотрудники должны иметь титульный лист со следующей записью для факсимильной передачи, содержащей информацию для ограниченного или внутреннего пользования, или при общении с третьими лицами (например, поставщик или консультант, участвующие в деятельности компании PepsiCo):

   «ДАННЫЙ ФАКС И ЕГО СОДЕРЖАНИЕ ПРЕДНАЗНАЧЕНЫ ТОЛЬКО ДЛЯ ПОЛЬЗОВАНИЯ АДРЕСУЕМЫМИ ПОЛУЧАТЕЛЯМИ И МОГУТ СОДЕРЖАТЬ ИНФОРМАЦИЮ, ЯВЛЯЮЩУЮСЯ СЛУЖЕБНОЙ, КОНФИДЕНЦИАЛЬНОЙ ИЛИ РЕГУЛИРУЕМОЙ ЗАКОНОМ ОБ АВТОРСКИХ ПРАВАХ. ЕСЛИ ВЫ НЕ ЯВЛЯЕТЕСЬ НАЗНАЧЕННЫМ ПОЛУЧАТЕЛЕМ ИЛИ АГЕНТОМ, ОТВЕТСТВЕННЫМ ЗА ДОСТАВКУ ДАННОГО ДОКУМЕНТА НАЗНАЧЕННОМУ ПОЛУЧАТЕЛЮ, НАСТОЯЩИМ ВЫ УВЕДОМЛЯЕТЕСЬ О ТОМ, ЧТО ЛЮБОЕ ИСПОЛЬЗОВАНИЕ, РАСПРОСТРАНЕНИЕ, РАСПРЕДЕЛЕНИЕ ИЛИ КОПИРОВАНИЕ ДАННОГО СООБЩЕНИЯ СТРОГО ЗАПРЕЩЕНО И МОЖЕТ БЫТЬ НЕЗАКОННЫМ. ЕСЛИ ВЫ ПОЛУЧИЛИ ДАННЫЙ ФАКС ПО ОШИБКЕ, СРАЗУ ЖЕ СООБЩИТЕ ОБ ЭТОМ ОТПРАВИТЕЛЮ ПО ФАКСУ ИЛИ ТЕЛЕФОНУ И УНИЧТОЖЬТЕ ФАКС, ОТПРАВЛЕННЫЙ ПО ОШИБКЕ».

   При необходимости Сотрудники могут изменять текст для соответствия местному языку и нормативным требованиям.

F. Право на осуществление контроля

1. Компания PepsiCo сохраняет за собой право на осуществление контроля, регистрации, разглашения, аудита и удаления типа и содержимого деятельности Сотрудника с применением ресурсов телефонной связи компании PepsiCo без предварительного уведомления.

G. Ожидания неприкосновенности частной жизни

1. Сотрудники не должны рассчитывать на то, что их частная жизнь останется неприкосновенной при использовании ресурсов телекоммуникаций компании PepsiCo.
2. Компания PepsiCo сохраняет за собой право определять, какие действия можно совершать с информацией, полученной в результате деятельности Сотрудника (например, сообщения, рабочий продукт и резервные средства), осуществляемой с применением компьютерных (например, телекоммуникации) ресурсов компании PepsiCo.

Действия могут включать, помимо прочего, разглашение характера и содержания деятельности сотрудникам правоохранительных органов или иным третьим лицам без предварительного уведомления Сотрудника. Деятельность Сотрудника может стать общедоступной.

H. Сообщение о неправильном использовании

1. Сотрудники должны сообщать о фактическом или предполагаемом неправильном использовании ресурсов телефонной связи компании PepsiCo и получении недопустимого содержимого в соответствии со *Стандартом по составлению отчетности о неправильном использовании*.
2. Сотрудники должны изменить пароль телекоммуникаций при обнаружении или возникновении подозрения о том, что кто-то еще знает данный пароль.
3. Сотрудники должны сразу же сообщить взломанные пароли в Центр технической поддержки компании PepsiCo или местный центр поддержки.

2.5 Стандарт по допустимому использованию компьютерного и программного обеспечения

Данный *Стандарт по допустимому использованию программного обеспечения* основан на целях, приведенных в *Правилах допустимого использования*, и содержит специальные требования к правильному и надлежащему использованию компьютерных и программных ресурсов (например, портативные компьютеры, рабочие станции, коммуникаторы и инструментарий для повышения производительности программного обеспечения).

2.5.1 Область применения

Настоящий стандарт относится к Сотрудникам, использующим компьютерные и программные ресурсы, принадлежащие компании PepsiCo.

2.5.2 Принятие ответственности за соблюдение

Использование Сотрудником компьютерных и программных ресурсов компании PepsiCo является четко выраженным согласием соблюдать настоящий *Стандарт по допустимому использованию компьютерного и программного обеспечения*.

2.5.3 Требования

A. Бизнес-применение

1. Сотрудники несут ответственность за работу, связанную с использованием компьютерных и программных ресурсов, предоставленных компанией PepsiCo.
2. Сотрудники должны защищать информацию для ограниченного и внутреннего пользования, доступ к которой предоставляется, которая обрабатывается и (или) хранится на компьютерных и программных ресурсах, в соответствии с требованиями *Политики защиты ресурсов*.

3. Сотрудники должны хранить записи о лицензиях на компьютерное и программное обеспечение и прилагаемую документацию.

   Также необходимо хранить документацию по программному обеспечению, используемому для получения технической поддержки, и программному обеспечению, дающему право на скидки при покупке обновлений.

4. Компьютерные и программные ресурсы компании PepsiCo приобретаются и используются для ведения официальной экономической деятельности компании PepsiCo в соответствии с действующими законами, правилами и лицензионными соглашениями.

5. Компания PepsiCo должна проверять соблюдение лицензионных соглашений по компьютерному и программному обеспечению в установленном порядке.

6. Компания PepsiCo разрешает Сотрудникам периодически использовать свои компьютерные и программные ресурсы в личных целях, при условии, что данное использование не оказывает неблагоприятного влияния на работу компании PepsiCo.

B. Ненадлежащее использование (включая, среди прочего, следующее):

1. Сотрудники не должны нарушать законы об авторском праве, о патентах, интеллектуальной собственности или любые иные действующие законы или лицензионные соглашения, относящиеся к компьютерному и программному обеспечению.

2. Сотрудники не должны использовать копии подлинников программного обеспечения, хранящиеся в архиве, для ведения обычных деловых операций.

3. Сотрудники не должны использовать, воспроизводить или распространять копии с подлинников или резервные копии программного обеспечения, если только это не разрешено лицензионным соглашением или Руководством филиала компании PepsiCo.

4. Сотрудники не должны использовать технологию обхода лицензионных соглашений по программному обеспечению.

5. Сотрудники не должны устанавливать программное обеспечение (например, игры или музыку), не относящееся к деятельности.

6. Компьютерные и программные ресурсы компании PepsiCo не должны использоваться для следующего:

   - Незаконная и ненадлежащая деятельность
   - Деятельность, влияющая на обычный ход работы компании
   - Деятельность, нарушающая Кодекс поведения или политики компании PepsiCo
   - Деятельность, препятствующая выполнению индивидуальной или иной работы сотрудником

7. Компьютерные и программные ресурсы компании PepsiCo не должны использоваться для получения доступа, передачи, получения, распечатывания или хранения любого изображения, графика, документа, текста или иного материала, который может рассматриваться иными лицами как приносящий беспокойство, унизительный, дискриминирующий или оскорбительный на основании их расовой, национальной принадлежности, цвета кожи, пола, сексуальной ориентации, возраста, ограниченных физических возможностей, статуса ветерана и религиозных или политических убеждений.

   Сотрудникам следует знать, что большое количество материалов может рассматриваться как приносящее беспокойство, унизительное, дискриминирующее или оскорбительное.

8. Компьютерные и программные ресурсы компании PepsiCo не должны использоваться для преднамеренного отключения или перегрузки любой системы или сети или для обхода системы, предназначенной для защиты информации Сотрудника и (или) компании PepsiCo.

9. Компьютерные и программные ресурсы компании PepsiCo не должны использоваться для навязывания услуг, рекламирования или ведения коммерческой деятельности, не связанной с деятельностью компании PepsiCo.

C. Загружаемый материал

1. Сотрудники должны соблюдать действующее законодательство об авторском праве и лицензионные соглашения для материалов (например, программное обеспечение, файлы, графики, документы, сообщения, музыка или видео), загружаемых посредством компьютерных и программных ресурсов компании PepsiCo.
2. Сотрудники не должны загружать материал, требующий наличия лицензии, платы за регистрацию или не относящийся к деятельности компании PepsiCo, без разрешения Руководства филиала компании PepsiCo.
3. Сотрудники не должны выгружать, загружать, отправлять, получать, хранить или распечатывать следующие материалы без разрешения Руководства филиала компании PepsiCo:

   ■ Программное обеспечение (например, бесплатное программное обеспечение, условно-бесплатное программное обеспечение, коммерческое или общедоступное программное обеспечение)
   ■ Внешний материал от лиц или компаний, неизвестных Сотруднику
   ■ Информация компании PepsiCo или правительственная информация, предназначенная для ограниченного пользования (примеры приведены в *Политике защиты ресурсов*)
4. Сотрудники должны соблюдать процедуры, утвержденные компанией PepsiCo, по сканированию загружаемого содержимого и приложений на наличие вирусов и иных вредоносных кодов в соответствии с требованиями, приведенными в *Политике защиты ресурсов.*

D. Право на осуществление контроля

1. Компания PepsiCo сохраняет за собой право на осуществление контроля, регистрации, разглашения, аудита и удаления типа и содержимого деятельности Сотрудника и программного обеспечения с применением компьютерных и программных ресурсов компании PepsiCo без предварительного уведомления.

E. Ожидания неприкосновенности частной жизни

1. Сотрудники не должны рассчитывать на то, что их частная жизнь останется неприкосновенной при использовании компьютерных и программных ресурсов компании PepsiCo.
2. Компания PepsiCo сохраняет за собой право определять, какие действия можно совершать с информацией, полученной в результате деятельности Сотрудника (например, установка программного обеспечения, сообщения, рабочий продукт и резервные средства), осуществляемой с применением компьютерных и программных ресурсов компании PepsiCo.

   Действия могут включать, помимо прочего, разглашение типа и содержания деятельности сотрудникам правоохранительных органов или иным третьим лицам без предварительного уведомления Сотрудника. Деятельность Сотрудника может стать общедоступной.

F. Сообщение о неправильном использовании

1. Сотрудники должны сообщать о фактическом или предполагаемом неправильном использовании компьютерных и программных ресурсов компании PepsiCo и получении недопустимого содержимого в соответствии со *Стандартом по составлению отчетности о неправильном использовании*.
2. Сотрудники должны изменить пароль компьютера и (или) программного обеспечения связи при обнаружении или возникновении подозрения о том, что кто-то еще знает данный пароль.
3. Сотрудники должны сразу же сообщить взломанные пароли в Центр технической поддержки компании PepsiCo или местный центр поддержки.

2.6 Стандарт по уведомлению о неправильном использовании

Данный *Стандарт по уведомлению о неправильном использовании* основан на целях, приведенных в *Правилах допустимого использования*, и содержит специальные требования к ведению отчетности о несоблюдении *Правил допустимого использования* и смежных стандартов.

2.6.1 Требования

A. Общие требования

1. Полное или частичное несоблюдение Сотрудником *Правил допустимого использования* и смежных стандартов является неправильным использованием, и о нем сообщается в течение 24 часов.

B. Уведомление о неправильном использовании

1. О неправильном использовании или предполагаемом неправильном использовании Сотрудником сообщается Руководству филиала компании PepsiCo и (или) местному представителю Отдела кадров или по анонимному телефонному номеру.
2. Сотрудники или иные лица, сообщающие о неправильном использовании, должны указать следующее:
   - Имя (имена) лица (лиц), осуществляющие неправильное использование
   - Конкретные подробности, относящиеся к неправильному использованию, включая дату, время и описание инцидента
3. Сотрудники не должны непосредственно обсуждать инцидент с лицом(-ами), осуществляющим(-и) неправильное использование, без разрешения Управления кадрами компании PepsiCo.

   Данный тип информации предоставляется по мере необходимости.
4. Компания PepsiCo должна по своему усмотрению и в соответствии с действующими законами соблюдать конфиденциальность лиц, сообщивших о неправильном использовании.

   Процесс разрешения вопросов, связанных с неправильным использованием или предполагаемым неправильным использованием, может управляться независимой сторонней организацией.

3 Подготовка и информированность о мерах безопасности

3.1 Политика подготовки и информирования о мерах безопасности

3.1.1 Программное заявление

Настоящая *Политика информирования о мерах безопасности* определяет цели компании PepsiCo по созданию Программы информирования о мерах безопасности и специальных стандартов по обучению, подготовке и доведению до сведения Концепции программы обеспечения информационной безопасности компании PepsiCo и смежных политик и стандартов по обеспечению информационной безопасности.

3.1.2 Цели

Концепция программы обеспечения информационной безопасности, политики и стандарты регулярно доводятся до сведения всех сотрудников компании PepsiCo и размещаются в корпоративной интрасети. В результате Сотрудники регулярно информируются о возникновении вопросов по информационной безопасности, тенденциях и рисках для информационных ресурсов компании PepsiCo.

Доступ к документации по процедурам обеспечения информационной безопасности, такой как технические стандарты, базовые конфигурации и подробные инструкции, предоставляется и ограничивается пользователями, которым данная информация необходима в связи с утвержденной производственной необходимостью или выполнения установленных рабочих обязанностей.

Сотрудники извещаются о внесении изменений, дополнений и исправлений в Концепцию программы обеспечения информационной безопасности, политики и стандарты.

Специальные требования к информированности о мерах безопасности, обучению, подготовке и средствам связи приведены в следующих Стандартах, относящихся к настоящей политике:

- *Стандарт по управлению информированием о мерах безопасности*
- *Стандарт по информированию Новых сотрудников о мерах безопасности*
- *Стандарт по информированию третьих лиц о мерах безопасности*

3.1.3 Обязанности

Руководство филиала компании PepsiCo несет ответственность за доведение до сведения и рассмотрение в своих организационных подразделениях *Политики подготовки и информирования о мерах безопасности* и смежных стандартов. Руководство филиала компании PepsiCo также несет ответственность за определение, утверждение и выполнение процедур по обеспечению соблюдения политики и стандартов.

Сотрудники несут ответственность за изучение и соблюдение *Политики подготовки и информирования о мерах безопасности* и смежных стандартов.

3.2 Стандарт по управлению информированием о мерах безопасности

Настоящий *Стандарт по управлению информированием о мерах безопасности* основан на целях, приведенных в *Политике подготовки и информирования о мерах безопасности*, и содержит специальные требования к информированию о мерах безопасности и подготовке руководства компании PepsiCo.

3.2.1 Область применения

Настоящий стандарт относится к Менеджерам (Сотрудникам с руководящими полномочиями).

3.2.2 Требования

A. Общие требования

1. Менеджеры должны пройти подготовку в области информационной безопасности.
2. При необходимости Менеджеры должны получать отчеты о событиях информационной безопасности.

B. Политики

1. Подготовка Менеджера в области информационной безопасности должна включать темы и стандарты, предусмотренные иными Сотрудниками и относящиеся к следующим политикам:
   - *Правила допустимого использования*
   - *Политика управления ресурсами*
   - *Политика подготовки и информирования о мерах безопасности*
   - *Политика оценки и контроля угроз*
   - *Политика оценки и управления уязвимостями*

C. Стандарты

1. Подготовка Менеджера в области информационной безопасности должна включать темы и стандарты, относящиеся к должностным обязанностям менеджера. Например:
   - *Стандарт шифрования*
   - *Стандарт по управлению изменениями*
   - *Стандарт по реагированию на инциденты*
   - *Стандарт по оценке угроз*
   - *Стандарт по защите от угроз доступности информации*
   - *Стандарт по оценке уязвимостей*
   - *Стандарт по управлению уязвимостями*

3.3 Стандарт по информированию новых Сотрудников о мерах безопасности

Данный *Стандарт по информированию новых Сотрудников о мерах безопасности* основан на целях, приведенных в *Политике подготовки и информирования о мерах безопасности*, и содержит специальные требования к информированию о мерах безопасности и подготовке Новых сотрудников компании PepsiCo.

3.3.1 Область применения

Настоящий стандарт относится к Новым сотрудникам, нанимаемым компанией PepsiCo.

3.3.2 Требования

A. Общие требования

1. Как часть адаптации новые Сотрудники должны пройти подготовку в области информационной безопасности, которая включает:
   - Концепцию программы обеспечения информационной безопасности компании PepsiCo
   - Направленность компании PepsiCo на обеспечение информационной безопасности
   - Обязанности Сотрудника по обеспечению информационной безопасности
   - Критические информационные ресурсы компании PepsiCo, относящиеся к установленным рабочим обязанностям

2. При необходимости Новые сотрудники должны получать отчеты о событиях информационной безопасности.

B. Политики

1. Подготовка Новых сотрудников в области информационной безопасности должна включать Концепцию программы обеспечения информационной безопасности компании PepsiCo и темы и стандарты, относящиеся к следующим политикам:

   - *Правила допустимого использования*
   - *Политика защиты ресурсов*
   - *Политика подготовки и информирования о мерах безопасности*
   - *Политика определения и классификации ресурсов*

2. Новые сотрудники, выполняющие обязанности Хранителя или Владельца информации, проходят подготовку в области обеспечения информационной безопасности, включая темы и стандарты, относящиеся к следующим политикам:

   - *Политика управления ресурсами*
   - *Политика оценки и контроля угроз*
   - *Политика оценки и управления уязвимостями*

C. Стандарты

1. Подготовка Нового сотрудника в области информационной безопасности должна включать темы и стандарты, относящиеся к должностным обязанностям Сотрудника. Например:

   - Критические информационные ресурсы, категории классификации конфиденциальности, маркировка и работа с информацией.
   - Средства управления физическим доступом, требования к учетным записям и паролям пользователя, удаленный доступ и мобильные компьютерные среды, профилактика и обнаружение вирусов и правильное использование программных и компьютерных систем.
   - Допустимое использование ресурсов компании PepsiCo, неправильное использование и сообщение об инциденте, связь с Центром технической поддержки компании PepsiCo (или местным центром поддержки) и контактные лица по вопросам информационной безопасности.

3.4 Стандарт по информированию третьих лиц о мерах безопасности

Настоящий *Стандарт по информированию третьих лиц о мерах безопасности* основан на целях, приведенных в *Политике подготовки и информирования о мерах безопасности*, и содержит специальные требования к информированию о мерах безопасности и подготовке Сторонних сотрудников.

3.4.1 Область применения

Настоящий стандарт относится к Сторонним сотрудникам, пользующимся информацией, системами, службами и (или) оборудованием компании PepsiCo.

3.4.2 Требования

A. Общие требования

1. В ходе ознакомления Сторонние сотрудники должны пройти подготовку в области информационной безопасности, которая включает:

   - Концепцию программы обеспечения информационной безопасности компании PepsiCo
   - Направленность компании PepsiCo на обеспечение информационной безопасности
   - Обязанности Стороннего сотрудника по обеспечению информационной безопасности

2. Подготовка Стороннего сотрудника в области информационной безопасности является выборочной.

Правила информационной безопасности компании PepsiCo являются частной собственностью компании и не должны передаваться Сторонним сотрудникам, если только данные правила необходимы для выполнения рабочих поручений.

B. Политики

1. Подготовка Сторонних сотрудников в области информационной безопасности должна включать Концепцию программы обеспечения информационной безопасности компании PepsiCo и темы и стандарты, относящиеся к следующим политикам:

   - *Правила допустимого использования*
   - *Политика защиты ресурсов*
   - *Политика определения и классификации ресурсов*

2. Сторонние сотрудники, выполняющие обязанности Хранителя информации, проходят подготовку в области обеспечения информационной безопасности, включая темы и стандарты, относящиеся к следующим политикам:

   - *Политика управления ресурсами*
   - *Политика оценки и контроля угроз*
   - *Политика оценки и управления уязвимостями*

C. Стандарты

1. Подготовка Стороннего сотрудника в области информационной безопасности должна включать темы и стандарты, относящиеся к должностным обязанностям Сотрудника. Например:

   - Требования к неразглашению, ограничение доступа по контракту, категории классификации конфиденциальности, маркировка и работа с информацией.
   - Средства управления физическим доступом, требования к учетным записям и паролям пользователя, удаленный доступ и мобильные компьютерные среды, профилактика и обнаружение вирусов и правильное использование программных и компьютерных систем.
   - Допустимое использование ресурсов компании PepsiCo, неправильное использование и сообщение об инциденте, связь с Центром технической поддержки компании PepsiCo (или местным центром поддержки) и контактные лица по вопросам информационной безопасности.

4 Оценка и контроль угроз

4.1 Политика оценки и контроля угроз

4.1.1 Программное заявление

Данная *Политика оценки и контроля угроз* определяет цели компании PepsiCo по созданию специальных стандартов оценки и последующего контроля угроз для информационных ресурсов компании PepsiCo.

4.1.2 Цели

Угрозы являются преднамеренными или случайными действиями или событиями, которые могут неблагоприятно влиять на информационные ресурсы компании PepsiCo, и источниками (например, отдельные лица, группы или организации) данных действий или событий.

Компания PepsiCo понимает, что невозможно полностью предотвратить возникновение инцидентов безопасности. Принципом реагирования компании PepsiCo является сдерживание угрозы, быстрое возобновление обслуживания и получение соответствующей информации о каждом инциденте. Для минимизации воздействия компания PepsiCo разрабатывает и реализует планы реагирования на инциденты. Специальные требования к обнаружению и реагированию на инциденты информационной безопасности приведены в *Стандарте по реагированию на инциденты*.

Для обеспечения надлежащего реагирования потенциальные угрозы для информационных ресурсов оцениваются и располагаются в порядке очередности. Специальные требования к оценке и приоритезации угроз приведены в *Стандарте по оценке угроз.*

Для обнаружения угрозы и проникновения необходимо осуществлять эффективный контроль безопасности. Специальные требования к контролю и обнаружению угроз приведены в *Стандарте по контролю угроз.*

4.1.3 Обязанности

Руководство филиала компании PepsiCo несет ответственность за доведение до сведения и рассмотрение в своих организационных подразделениях *Политики оценки и контроля угроз* и смежных стандартов. Руководство филиала компании PepsiCo также несет ответственность за определение, утверждение и выполнение процедур по обеспечению соблюдения политики и стандартов.

Сотрудники несут ответственность за изучение и соблюдение *Политики оценки и контроля угроз* и смежных стандартов.

4.2 Стандарт по реагированию на инциденты

Настоящий *Стандарт по реагированию на инциденты* основан на целях, приведенных в *Политике оценки и контроля угроз*, и содержит специальные требования к реагированию на инциденты информационной безопасности.

4.2.1 Требования

A. Общие требования

1. Сотрудники должны сразу же сообщать об инцидентах информационной безопасности в Центр технической поддержки компании PepsiCo или местный центр поддержки.

Опасения по поводу сообщения о возникновении инцидента можно обсудить с Руководителем филиала компании PepsiCo или представителем Отдела кадров. При необходимости анонимного сообщения можно воспользоваться телефонным номером анонимной горячей линии компании PepsiCo.

2. Руководство филиала компании PepsiCo должно рассмотреть инциденты информационной безопасности и предполагаемые инциденты.

   Реагирование на инцидент зависит от фактических или потенциальных неблагоприятных последствий для деятельности компании.

3. Группа(-ы) реагирования на инциденты информационной безопасности компании PepsiCo должна(-ы) поддерживать связь с филиалами компании PepsiCo, для которых инцидент имел последствия.
4. Группа(-ы) реагирования на инциденты информационной безопасности компании PepsiCo должна(-ы) выполнять все необходимые действия по управлению инцидентом (т.е. начиная с превентивного планирования и заканчивая последующим реагированием).
5. Группа(-ы) реагирования на инциденты информационной безопасности компании PepsiCo ведут документацию, включающую информацию об инциденте, меры по реагированию и причины возникновения инцидента.

B. Требования к реагированию

1. Руководство филиала компании PepsiCo назначает старшего менеджера с полномочиями принимать решения о реагировании на инцидент для выполнения деловых операций.
2. Группа(-ы) реагирования на инциденты информационной безопасности компании PepsiCo должна(-ы) разработать корпоративную классификацию серьезности инцидента, эскалации и реагирования.
3. Группа(-ы) реагирования на инциденты информационной безопасности компании PepsiCo должна(-ы) сообщать о состоянии реагирования Руководству филиала компании PepsiCo, а при необходимости и CISO.
4. Возможности реагирования на инциденты информационной безопасности компании PepsiCo должны проверяться как минимум один раз в год.

   Проверка возможности реагирования на инцидент планируется для проведения оценки и непрерывного улучшения.

C. Разглашение информации об инциденте

1. Сотрудники не должны предоставлять информацию, относящуюся к безопасности, любым средствам массовой информации или внешнему источнику, кроме как через Отдел по связям с общественностью компании PepsiCo и при наличии разрешения Функционального вице-президента компании PepsiCo.
2. Информация компании PepsiCo, относящаяся к безопасности, может разглашаться только по мере служебной необходимости.

4.3 Стандарт по оценке угроз

Данный *Стандарт по оценке угроз* основан на целях, приведенных в *Политике оценки и контроля угроз*, и содержит специальные требования к оценке и приоритезации угроз.

4.3.1 Требования

A. Оценка

1. Действия компании PepsiCo по управлению рисками должны включать оценку угроз для систем и сетей, хранящих, обрабатывающих и (или) передающих информационные ресурсы компании PepsiCo.
2. Оценка угроз компании PepsiCo должна иметь комплексный подход к обнаружению, оценке, классификации и приоритезации потенциальных угроз. Примеры размеров анализа угроз включают:

   - Стоимость (например, потенциальная стоимость защиты, реагирования и восстановления)
   - Источник (например, внутренний в сравнении с внешним и достоверный в сравнении с недостоверным)
   - Мотивация (например, злонамеренный, криминальный, случайный и естественный)
   - Последствия (например, потеря конфиденциальности, целостности и (или) доступности)
   - Тип (например, «червь», вирус, социальный инжиниринг и отказ в обслуживании)
   - Воздействие (например, специальные информационные ресурсы, которые являются целью или на которые можно воздействовать)
   - Очевидность/профиль (например, низкая, средняя или высокая степень риска публичного представления или воздействия на репутацию компании)

B. Приоритезация

1. Угрозы для компании PepsiCo должны располагаться в порядке очередности в соответствии с вероятностью наступления события. Шкала оценки приоритезации угрозы может включать:

   - Высокий уровень (Категория 1)
   - Средний уровень (Категория 2)
   - Низкий уровень (Категория 3)

2. Угрозы для компании PepsiCo должны распределяться по категориям для проведения оценки. Схема распределения угроз по категориям может включать:

   - Тип угрозы
   - Очевидность угрозы
   - Финансовые последствия
   - Конфиденциальность данных
   - Наличие уязвимости, на которую может быть направлена угроза

4.4 Стандарт по контролю угроз

Настоящий *Стандарт по контролю угроз* основан на целях, приведенных в *Политике оценки и контроля угроз*, и содержит специальные требования к осуществлению контроля угроз, включая автоматическое и ручное обнаружение, рассмотрение и анализ информации, а также отслеживание и информирование о метрических показателях.

4.4.1 Требования

A. Общие требования

1. Сотрудники должны контролировать системы и сети на основании их важности для деятельности, доступности (например, через сеть Интернет) и (или) приоритезации угроз.
2. Сотрудники должны разрабатывать процедуры быстрого реагирования на возникновение инцидентов безопасности.
3. Компания PepsiCo должна указать обязанности поставщиков услуг в контрактах на оказание услуг по контролю безопасности сторонними организациями (например, контракты с Поставщиком услуг по управлению информационной безопасностью).

B. Обнаружение вручную

1. Сотрудники должны разработать процедуры обнаружения инцидента вручную и проверки журнала для критических систем и сетей.

   Процедуры дополнят систему автоматического контроля безопасности и процессы или обеспечат осуществление контроля безопасности там, где автоматические процессы неприменимы.

C. Рассмотрение и анализ информации

1. Сотрудники должны проверять и анализировать информацию об угрозах, полученную из внешних источников (например, Поставщики услуг по управлению информационной безопасностью), для информирования относительно угроз информационной безопасности.

D. Отслеживание и информирование о метрических показателях

1. Руководство филиала компании PepsiCo должно контролировать свою информацию об угрозах и регулярно представлять отчеты о состоянии CISO. Отчеты о состоянии должны включать следующую информацию:

   - Анализ тенденций изменения угроз
   - Возникающие угрозы (например, «черви»)
   - Типы инцидентов и соответствующие угрозы (например, количество и серьезность)

5 Оценка и управление уязвимостями

5.1 Политика оценки и управления уязвимостями

5.1.1 Программное заявление

Настоящая *Политика оценки и управления уязвимостями* определяет цели компании PepsiCo по созданию специальных стандартов по оценке и непрерывному управлению уязвимостями информационных ресурсов компании PepsiCo.

5.1.2 Цели

Компания PepsiCo регулярно оценивает и определяет уязвимости в средствах контроля, защищающих ее системы, сети и информационные ресурсы. Специальные требования к оценке уязвимостей приведены в *Стандарте по оценке уязвимостей.*

Планы для программ непрерывного смягчения уязвимостей должны включать результаты оценки уязвимостей. Через какое-то время компания PepsiCo разработает соответствующие метрические показатели для измерения эффективности данных программ. Специальные требования к управлению уязвимостями приведены в *Стандарте по управлению уязвимостями.*

5.1.3 Обязанности

Руководство филиала компании PepsiCo несет ответственность за доведение до сведения и рассмотрение в своих организационных подразделениях *Политики оценки и управления уязвимостями* и смежных стандартов. Руководство филиала компании PepsiCo также несет ответственность за определение, утверждение и выполнение процедур по обеспечению соблюдения политики и стандартов.

Сотрудники несут ответственность за изучение и соблюдение *Политики оценки и управления уязвимостями* и смежных стандартов.

5.2 Стандарт по оценке уязвимостей

Настоящий *Стандарт по оценке уязвимостей* основан на целях, приведенных в *Политике оценки и управления уязвимостями*, и содержит специальные требования к оценке и приоритезации уязвимостей.

5.2.1 Требования

A. Оценка

1. Действия компании PepsiCo по управлению рисками должны включать оценку уязвимостей для систем и сетей, хранящих, обрабатывающих и (или) передающих информационные ресурсы компании PepsiCo.

Очередность проведения оценок работы системы и сети определяется согласно их важности для деятельности.

2. Сотрудники должны регулярно проверять системы и сети на наличие уязвимостей.

Выборка является одним из методов проверки и включает проверку типовой системы или сети на наличие уязвимостей и экстраполирование результатов для применения к аналогичным системам и сетям.

3. При необходимости Сотрудники должны предпринимать следующие действия при проведении оценок сетевой уязвимости:

   ■ Проверка на наличие пропущенных или устаревших заплат
   ■ Проверка сетей на наличие известных уязвимостей
   ■ Тестирование сервисных портов для определения несанкционированных сервисов

4. При необходимости Сотрудники должны предпринимать следующие действия при проведении оценок уязвимости технологического сервера:

   - Проверка серверов на наличие известных уязвимостей.
   - Проверка конфигураций сервера, чтобы убедиться в том, что они утверждены компанией PepsiCo.
   - Проверка инвентарных списков системы и сервера для определения лишних или самовольных установок.
   - Проверка конфигураций аудитирования, чтобы убедиться в том, что события безопасности регистрируются в соответствии с требованиями, приведенными в *Стандарте по аудиту*.
   - Проверка средств защиты относительно информации, предназначенной для ограниченного пользования, чтобы убедиться в том, что они укомплектованы и применяются в соответствии с требованиями, приведенными в *Стандарте шифрования*.
   - Проверка сервера и средств резервирования данных, чтобы убедиться в том, что они укомплектованы и применяются в соответствии с требованиями, приведенными в *Стандарте по защите от угроз доступности информации*.
   - Проверка критических директорий сервера и средств управления доступом на уровне файлов, чтобы убедиться в том, что они укомплектованы и применяются в соответствии с требованиями, приведенными в *Стандарте по управлению доступом.*
   - Проверка средств управления идентификацией и аутентификацией относительно идентификаторов пользователей и учетных записей сервера, чтобы убедиться в том, что они укомплектованы и применяются в соответствии с требованиями, приведенными в *Стандарте по управлению доступом*.

5. При необходимости Сотрудники должны предпринимать следующие действия при проведении оценок уязвимости бизнес-системы:

   - Проверка системы на наличие известных уязвимостей. Примеры включают:
     ✓ Средства управления доступом
     ✓ Средства управления базой данных
     ✓ Средства управления шифрованием
     ✓ Управление сеансами
     ✓ Безопасность со стороны клиента
   - Проверка систем для определения, надлежащим ли образом они реагируют на недействительные или поврежденные входные значения.
   - Проверка средств защиты систем, которые хранят, обрабатывают и (или) передают информацию, предназначенную для ограниченного пользования, чтобы убедиться в том, что они укомплектованы и применяются в соответствии с требованиями, приведенными в *Стандарте по управлению доступом*.
   - Проверка средств управления идентификацией и аутентификацией относительно систем, предоставляющим доступ к информационным ресурсам компании PepsiCo, чтобы убедиться в том, что они укомплектованы и применяются в соответствии с требованиями, приведенными в *Стандарте по управлению доступом* и *Стандарте шифрования*.

6. Сотрудники должны оценивать уязвимость информационных ресурсов системы до развертывания производства.

   Обнаруженные уязвимости должны быть устранены до начала развертывания.

7. Сотрудники должны оценивать уязвимость информационных ресурсов системы после того, как в ней произойдут существенные изменения.

8. Сотрудники должны оценивать уязвимость объектов, содержащих системы, которые хранят, обрабатывают и (или) передают информацию, предназначенную для ограниченного пользования, чтобы убедиться в том, что средства управления физическим доступом укомплектованы и применяются в соответствии с требованиями, приведенными *Стандарте по предоставлению физического доступа*.

9. Компания PepsiCo должна определять очередность результатов оценки уязвимости на основании эксплуатационного риска и возможного неблагоприятного воздействия на информационные ресурсы компании PepsiCo. Ниже приведен пример матрицы оценок уязвимости:

Оценка уязвимости	Описание	Потенциальное воздействие
Высокая степень риска	Уязвимости, которые могут использоваться угрозами и представлять непосредственную опасность для информационной безопасности, систем или сетей.	Серьезное
Средняя степень риска	Уязвимости, которые могут привести к последующему проникновению и оказать существенное воздействие.	Ограниченное
Низкая степень риска	Уязвимости, которые вряд ли могут использоваться в данный момент, но на которые следует обратить внимание.	Незначительное

5.3 Стандарт по управлению уязвимостями

Настоящий *Стандарт по управлению уязвимостями* основан на целях, приведенных в *Политике оценки и управления уязвимостями*, и содержит специальные требования к действиям по управлению уязвимостями в закрытом контуре, включая смягчение уязвимости, рассмотрение и анализ информации, а также отслеживание и информирование о метрических показателях.

5.3.1 Требования

A. Смягчение

1. Сотрудники должны контролировать угрозы и источники угроз, которые могут использовать уязвимости высокой степени риска до их смягчения.
2. Сотрудники должны проверять решение вопросов, связанных с уязвимостью, после выполнения плана по устранению.
3. Руководство филиала компании PepsiCo должно устанавливать сроки устранения уязвимостей на основании присвоенной оценки уязвимости и оценок деловых рисков.

CISO содействует определению требований к устранению и (или) сроков для некоторых серьезных уязвимостей.

4. Планы компании PepsiCo по устранению уязвимостей должны включать предлагаемые решения по определенным уязвимостям, необходимые задачи для воздействия на изменения и определение необходимых задач для соответствующего персонала.
5. CISO или уполномоченное лицо утверждают отказы относительно уязвимости в установленном порядке.

   Отказы относительно уязвимости должны соответствовать ранее определенным критериям исключения. В некоторых исключительных случаях очень сложно устранить уязвимости (т.е. определенные приложения могут не работать при наложении заплат). В таких случаях оценка риска определяет соответствующие процедуры смягчения (например, заблокировать порты, отключить сервисы или ограничить маршрутизацию).

B. Рассмотрение и анализ информации

1. Сотрудники должны ежедневно проверять соответствующую информацию по уязвимости (например, сигналы тревоги), полученную из внутренних источников, от поставщиков услуг, исследований сторонних организаций и общих ресурсов.
2. Сотрудники должны распространять соответствующую информацию по уязвимостям среди заинтересованных сторон в установленном порядке.

Некоторые заинтересованные стороны включают Отдел информационной безопасности, Отдел по управлению рисками и корпоративному аудиту и сотрудников Отдела информационных технологий, таких как PBSG.

C. Отслеживание и информирование о метрических показателях

1. Сотрудники должны отслеживать метрические показатели управления уязвимостью для составления отчетов по производительности и исполнению требований.

   Метрические показатели включают количество задач, поставленных для новых, закрытых или просроченных уязвимостей.

2. Руководство филиала компании PepsiCo ежеквартально сообщает результаты управления уязвимостью CISO, вице-президенту PBSG и главному техническому директору PBSG компании PepsiCo. Отчеты должны содержать следующие данные:

   - Степень серьезности уязвимостей
   - Количество уязвимостей за текущий квартал
   - Количество уязвимостей, открытых за текущий квартал
   - Количество уязвимостей, закрытых за текущий квартал
   - Количество исключений уязвимости за текущий квартал

6 Определение и классификация ресурсов

6.1 Политика определения и классификации ресурсов

6.1.1 Программное заявление

Настоящая *Политика определения и классификации ресурсов* определяет цели компании PepsiCo по созданию специальных стандартов по определению, классификации, обозначению и решению вопросов, связанных с информационными ресурсами компании PepsiCo.

6.1.2 Цели

Компания PepsiCo определяет уровень секретности информации на основании конфиденциальности и бизнес-ценности информации. Все информационные ресурсы, созданные внутри или вне компании, распределяются по одному из следующих уровней секретности информации:

- Для ограниченного пользования
- Только для внутреннего пользования
- Общедоступная

Если объединяется информация, относящаяся к разным уровням секретности, то итоговая совокупность информации или новая информация классифицируется по наиболее ограничивающему уровню источников. Специальные требования к определению уровней секретности информационных ресурсов приведены в *Стандарте по уровням секретности информации*.

Информация, предназначенная для ограниченного пользования, маркируется соответствующим обозначением уровня секретности информации и обрабатывается соответствующим образом. Такие обозначения должны указываться при любом раскрытии информации. Специальные требования к обозначению информационных ресурсов приведены в *Стандарте по обозначению и обращению информации*.

По возможности уровни секретности информации компании PepsiCo используются для управления решениями по защите информации (т.е. наряду с оценками риска, проектированием систем безопасности и т.д.).

6.1.3 Обязанности

Сотрудники обязаны отчитываться за следующие уровни ответственности при использовании информационных ресурсов компании PepsiCo:

1. Владельцы информации являются менеджерами организационных подразделений, которые несут основную ответственность за информационные ресурсы, связанные с их функциональными полномочиями. Если Владельцы информации неясно указаны в организационной модели, владение информацией передается CISO.

   Владельцы информации несут ответственность за:

   ■ Личные данные
   ■ Присваивание правильного уровня секретности информации
   ■ Обеспечение правильного обозначения информации, предназначенной для ограниченного пользования
   ■ Назначение Хранителя, владеющего информацией
   ■ Обеспечение ознакомления Хранителя с уровнями секретности информации
   ■ Регулярную проверку информации для определения необходимости изменения уровня секретности информации

2. Хранителями являются менеджеры, администраторы и иные лица, назначенные Владельцами информации для управления, обработки или хранения информационных ресурсов.
   Хранители несут ответственность за:

   ■ Осведомленность об уровнях секретности информации
   ■ Разработку и внедрение эффективных средств управления при необходимости
   ■ Применение необходимых средств управления (указанных в *Политике защиты ресурсов*) для защиты конфиденциальности, целостности и доступности информации
   ■ Применение необходимых средств управления (указанных в *Политике защиты ресурсов*) для поддержания и сохранения требований к уровням секретности и обозначению информации, установленных Владельцами информации

3. Сотрудниками являются отдельные лица, группы или организации, уполномоченные Владельцами информации для доступа к информационным ресурсам.
   Сотрудники несут ответственность за:

   ■ Осведомленность об уровнях секретности информации
   ■ Соблюдение средств управления, применяемых Хранителями
   ■ Связь с Владельцами информации, если информация не обозначена или неизвестен уровень секретности
   ■ Поддержание и сохранение требований к уровням секретности и обозначению информации, установленных Владельцами информации

6.2 Стандарт по уровням секретности информации

Настоящий *Стандарт по уровням секретности информации* основан на целях, приведенных в *Политике определения и классификации ресурсов*, и содержит специальные требования к классификации, переклассификации и исключению информационных ресурсов из классификации.

6.2.1 Требования

A. Конфиденциальность

1. Информация компании PepsiCo относится к одной из трех категорий конфиденциальности. Существуют следующие уровни секретности:

Уровни секретности	Описание	Примеры
Для ограниченного пользования	Коммерческая информация, являющаяся важной для деятельности компании PepsiCo, и информация, предусматривающая применение ограничения в связи с предписанием. Информация, предназначенная для ограниченного пользования, предусматривает особую осторожность при предоставлении доступа, передаче и хранении.	Примеры могут включать: • **Коммерческие тайны:** Формулы, рецепты, деловые практики/методы и схема ценообразования • **Ценная личная информация:** Номер соцстрахования, данные о заработной плате, данные о недееспособности, личностно-профессиональный рост сотрудника и закрытая медицинская информация • **Безопасность:** Пароли, PIN-коды, ключи шифрования и код критического источника/выполняемой программы

Уровни секретности	Описание	Примеры
Только для внутреннего пользования	Информация с возможностью доступа и использования в пределах компании PepsiCo. Доступ в пределах компании PepsiCo ограничивается по умолчанию; доступ предоставляется на основании производственной необходимости.	Примеры могут включать: • Списки телефонных номеров и телефонные справочники • Схемы организации • Политики и стандарты компании PepsiCo
Общедоступная	Информация с возможностью свободного доступа любого лица в любое время. Широко распространен незначительный деловой риск для данной информации.	Примеры могут включать: • Ежегодные отчеты компании PepsiCo • Каталоги изделий • Сообщения для прессы

2. Производственная коммерческая информация третьей стороны, которая назначена компанией PepsiCo на должность хранителя, классифицируется как информация, предназначенная для ограниченного пользования.
3. Информация компании PepsiCo по умолчанию относится к информации, предназначенной только для внутреннего пользования.
4. Информация компании PepsiCo, предназначенная для ограниченного пользования, обозначается выражением «Для ограниченного пользования» (которое должно быть читаемым) и остается в данной категории до тех пор, пока уровень секретности не будет изменен или информация не будет уничтожена.
5. Информация компании PepsiCo, предназначенная для ограниченного пользования, остается информацией, предназначенной для ограниченного пользования, при сочетании с информацией, предназначенной только для внутреннего пользования, или общедоступной информацией.
6. Информация компании PepsiCo, предназначенная только для внутреннего пользования, остается информацией, предназначенной только для внутреннего пользования, при сочетании с общедоступной информацией.

B. Доступность

1. Информация компании PepsiCo относится к одной из трех категорий доступности на основании возможных неблагоприятных последствий потери права доступа к данной информации. Уровни секретности следующие:
   - Высокий
   - Средний
   - Низкий
2. Руководство филиала компании PepsiCo должно синхронизировать уровни секретности информации по доступности с местными Планами устойчивости функционирования и послеаварийного восстановления.

C. Целостность

1. Руководство филиала компании PepsiCo должно разрабатывать процессы регулярной проверки целостности информации.

   Информация должна быть полной, точной, проверяемой и восстанавливаемой.

6.3 Стандарт по обозначению и обращению с информацией

Настоящий *Стандарт по обозначению и обращению с информацией* основан на целях, приведенных в *Политике защиты ресурсов*, и содержит специальные требования к обозначению и обращению с информационными ресурсами, передаваемыми или хранящимися в электронном или печатном виде.

6.3.1 Требования

A. Электронная информация

1. Сотрудники должны соблюдать требования к доступу, хранению и передаче электронной информации, приведенные в *Стандарте по уровням секретности информации*, *Стандарте по управлению доступом*, *Стандарте по предоставлению физического доступа* и *Стандарте шифрования*.
2. Владельцы информации должны разрешать разглашение электронной информации, предназначенной для ограниченного пользования, по мере необходимости.

B. Печатная информация

1. Сотрудники должны использовать уровни секретности печатной информации в соответствии с требованиями, приведенными в *Стандарте по уровням секретности информации*.
2. Сотрудники должны гарантировать, что печатная информация собирается и управляется (т.е. распространяется или уничтожается) в соответствии с требованиями к обращению.
3. Сотрудники должны управлять печатной информацией способом, соответствующим уровням секретности исходной информации:

Общедоступная	Только для внутреннего пользования	Для ограниченного пользования
Может физически храниться у всех на виду. Может свободно распространяться. Требования к уничтожению отсутствуют.	Не должна храниться у всех на виду. Может свободно распространяться среди сотрудников компании PepsiCo, если не предусмотрено иное. Уничтожается путем измельчения.	Обозначается как «Для ограниченного пользования». Не должна храниться у всех на виду и должна запираться, если не используется. Не должна копироваться, если только это не разрешено Владельцем информации. Уничтожается путем измельчения, сжигания или склеивания.

7 Защита ресурсов

7.1 Политика защиты ресурсов

7.1.1 Программное заявление

Настоящая *Политика защиты ресурсов* определяет цели компании PepsiCo по созданию специальных стандартов по защите конфиденциальности, целостности и доступности информационных ресурсов компании PepsiCo.

7.1.2 Цели

Предоставление права доступа к информации должно быть основано на уровне секретности информации и определено для обеспечения уровня доступа, необходимого для соответствия утвержденной производственной необходимости или выполнения установленных рабочих обязанностей. Необходима правильная идентификация и аутентификация. Политикой компании PepsiCo является присвоение уникального идентификатора всем Сотрудникам, устройствам и автоматизированным процессам до того, как данный Сотрудник, устройство или автоматизированный процесс получит доступ к любой информации, которая не является общедоступной. Специальные требования к контролю доступа к информационным ресурсам приведены в *Стандарте по управлению доступом*.

Предоставление права удаленного доступа к информационным ресурсам должно предоставляться только для соответствия утвержденной производственной необходимости или выполнения установленных рабочих обязанностей. Только методы и программы, утвержденные компанией PepsiCo, могут предоставлять удаленный доступ. Специальные требования к предоставлению удаленного доступа к информационным ресурсам приведены в *Стандарте по предоставлению удаленного доступа*.

Средства управления физическим доступом должны существовать в зонах, содержащих информационные ресурсы, или при проведении компьютерной обработки информации. Средства управления физическим доступом должны соответствовать уровню средств управления, необходимому для защиты информационных ресурсов и предоставления уровня доступа, необходимого Сотруднику для выполнения установленных рабочих обязанностей. Специальные требования к предоставлению физического доступа к информационным ресурсам приведены в *Стандарте по предоставлению физического доступа*.

Шифрование используется при передаче конфиденциальной информации через незащищенную или общедоступную сеть. Шифрование используется в соответствии с законодательством, а также должно использоваться для защиты конфиденциальной информации. Только алгоритмы и программы шифрования, утвержденные компанией PepsiCo, могут защитить информацию, предназначенную для ограниченного пользования. Специальные требования к шифрованию информационных ресурсов приведены в *Стандарте шифрования*.

Доступность информационных ресурсов является крайне важной для осуществления деятельности. При необходимости осуществляется планирование устойчивости функционирования для эффективного резервирования, дублирования и восстановления информационных ресурсов. Специальные требования к защите доступности информационных ресурсов приведены в *Стандарте по защите от угроз доступности информации*.

Антивирусы должны использоваться для защиты информационных ресурсов от разрушающих программных компонентов, таких как вирусы и иные вредоносные коды, которые препятствуют ведению нормальной деятельности. Антивирусные программы, утвержденные компанией PepsiCo, должны устанавливаться, включаться и обновляться на всех системах, подверженных заражению. Специальные требования к защите информационных ресурсов от вирусов и иных вредоносных кодов приведены в *Стандарте по антивирусной защите*.

Аудиторский инструментарий, отслеживающий перемещение или доступ к информации, включается для регистрации событий безопасности. Журналы аудита хранятся в надежном месте в течение определенного периода времени. Специальные требования к проверке информационных ресурсов приведены в *Стандарте по аудиту*.

7.1.3 Обязанности

Сотрудники обязаны отчитываться за следующие уровни ответственности при использовании информационных ресурсов компании PepsiCo:

1. Владельцы информации являются менеджерами организационных подразделений, которые несут основную ответственность за информационные ресурсы, связанные с их функциональными полномочиями. Если Владельцы информации неясно указаны в организационной модели, владение информацией передается CISO.

   Владельцы информации несут ответственность за:
   ■ Обеспечение конфиденциальности, целостности и доступности информации
   ■ Разрешение доступа к информации лицам, имеющим производственную необходимость
   ■ Определение процедур, соответствующих требованиям *Политики защиты ресурсов*
   ■ Отмена доступа к информации для лиц, которые больше не имеют производственной необходимости

2. Хранителями являются менеджеры, администраторы и иные лица, назначенные Владельцами информации для управления, обработки или хранения информационных ресурсов.
   Хранители несут ответственность за:

   ■ Разработку и внедрение эффективных средств управления при необходимости
   ■ Управление доступом к информации в соответствии с полномочиями, предоставленными Владельцами информации
   ■ Обеспечение безопасной среды обработки, защищающей конфиденциальность, целостность и доступность информации
   ■ Реализацию процессуальных гарантий, определенных Владельцами информации, в соответствии с требованиями, приведенными в *Политике защиты ресурсов*

3. Сотрудниками являются отдельные лица, группы или организации, уполномоченные Владельцами информация для доступа к информационным ресурсам.
   Сотрудники несут ответственность за:

   ■ Использование информации только по назначению
   ■ Соблюдение средств управления, применяемых Хранителями
   ■ Обращение к Владельцам информации, если информация не обозначена или неизвестен уровень секретности
   ■ Обеспечение конфиденциальности, целостности и доступности информации в соответствии с требованиями, приведенными в *Политике защиты ресурсов*.

7.2 Стандарт по управлению доступом

Настоящий *Стандарт по управлению доступом* основан на целях, приведенных в *Политике защиты ресурсов*, и содержит специальные требования к контролю идентификации, аутентификации и авторизации, необходимые для получения доступа к информационным ресурсам компании PepsiCo.

7.2.1 Требования

A. Общие требования

1. Системы компании PepsiCo, хранящие информацию, которая классифицируется как информация, предназначенная только для внутреннего или для ограниченного пользования, должны:

   ■ Идентифицировать и аутентифицировать Сотрудников
   ■ Регистрировать идентификатор, дату и время доступа
   ■ Отклонять совместно используемые или анонимные учетные записи
   ■ Обеспечивать доступность информации только для уполномоченных лиц
   ■ Вести учет уполномоченных Сотрудников и их текущих прав доступа

2. Системы компании PepsiCo, хранящие информацию, которая классифицируется как информация, предназначенная для ограниченного пользования, также должны:

   ■ Регистрировать неудачные попытки доступа
   ■ Копировать журналы аудита на главный компьютер централизованного журнала
   ■ Вести журналы аудита критических событий безопасности
   ■ Синхронизировать системные часы для обеспечения точности журнала

3. Сотрудники классифицируют информацию аутентификации (т.е. файлы паролей или пароли) как информацию, предназначенную для ограниченного пользования.

   Информация аутентификации должна защищаться во время хранения и передачи соответствующими средствами обеспечения конфиденциальности.

4. При входе в систему Сотрудники должны отображать баннер на операционных системах и сетевом оборудовании компании PepsiCo, если это позволяет программное обеспечение системы. Ниже приведен баннер входа в систему, утвержденный компанией PepsiCo:

   «ДАННАЯ СИСТЕМА И ВСЯ СООТВЕТСТВУЮЩАЯ ИНФОРМАЦИЯ, К КОТОРОЙ ПРЕДОСТАВЛЯЕТСЯ ДОСТУП, ЯВЛЯЕТСЯ СОБСТВЕННОСТЬЮ КОМПАНИИ PEPSICO INC. И ПРЕДНАЗНАЧЕНА ДЛЯ ИСПОЛЬЗОВАНИЯ ЛИЦАМИ, УПОЛНОМОЧЕННЫМИ КОМПАНИЕЙ PEPSICO. ПРОДОЛЖАЮЩЕЕСЯ ИСПОЛЬЗОВАНИЕ ДАННОЙ СИСТЕМЫ ПОДРАЗУМЕВАЕТ СОГЛАСИЕ НА ОСУЩЕСТВЛЕНИЕ КОНТРОЛЯ И ПОНИМАНИЕ ТОГО, ЧТО ЗАПИСЬ И (ИЛИ) РАЗГЛАШЕНИЕ ЛЮБЫХ ДАННЫХ СИСТЕМЫ МОЖЕТ ОСУЩЕСТВЛЯТЬСЯ ТОЛЬКО ПО УСМОТРЕНИЮ КОМПАНИИ PEPSICO».

   При необходимости Сотрудники могут изменять текст для соответствия местному языку и нормативным требованиям.

B. Идентификация

1. Сотрудники должны соблюдать данные правила идентификации для использования системы:
   ■ Создание идентификатора должно соответствовать соглашениям о наименованиях, утвержденным компанией PepsiCo
   ■ Уникальный идентификатор пользователя и пароль являются нормой учетных данных для проверки подлинности
   ■ Строгая двухфакторная аутентификация (т.е. электронные или аппаратные ключи и биометрические характеристики) может использоваться как расширенные учетные данные для проверки подлинности с целью защиты сверхконфиденциальной информации

2. Сотрудники не должны коллективно использовать секретную часть учетных данных для проверки подлинности (например, пароль или PIN-код).

3. Сотрудники должны создавать как можно большее количество учетных данных для проверки подлинности, необходимые для Сотрудника, устройства или автоматизированного процесса, но все учетные данные для проверки подлинности должны относиться только к одному Сотруднику, устройству или автоматизированному процессу.

   Учетные данные для проверки подлинности могут использоваться в многоуровневых системах и приложениях.

4. Учетные данные Сотрудников, не являющихся сотрудниками компании PepsiCo, для проверки подлинности должны содержать атрибуты, определяющие их как лиц, не являющихся сотрудниками компании.

5. Компания PepsiCo должна разрешать проведение одновременных сеансов в многоуровневых системах и приложениях.

6. Системы компании PepsiCo, предусматривающие аутентификацию, не должны раскрывать никакую информацию о системе до тех пор, пока аутентификация не будет успешно завершена.

C. Стандарты по аутентификации для Сотрудников

1. Сотрудники должны создавать пароли, соответствующие требованиям системы аутентификации.

2. Сотрудники должны обеспечивать конфиденциальность своих учетных данных для проверки подлинности и не разглашать секретную часть учетных данных для проверки подлинности (например, пароль или PIN-код).

Сотрудники не должны использовать один и тот же пароль для внутренних систем компании PepsiCo и внешних систем, не контролируемых компанией PepsiCo.

3. Сотрудники должны принимать разумные меры предосторожности в отношении кражи или потери любого маркера аутентификации, выданного компанией PepsiCo, и сразу же сообщать о любой краже или потери в Центр технической поддержки компании PepsiCo или местный центр поддержки.
4. Сотрудники должны изменять секретную часть учетных данных для проверки подлинности сразу же после ее разглашения или предполагаемого разглашения.
5. Сотрудники несут ответственность за любые действия, осуществляемые с их учетными данными для проверки подлинности.
6. Сотрудники должны извещаться о любом изменении, внесенном в их учетные данные для проверки подлинности.
7. Сотрудники должны получать новые учетные данные для проверки подлинности безопасным способом (например, запечатанный конверт).
8. Сотрудники не должны показывать или распечатывать пароли.
9. Сотрудники не должны жестко задавать пароли в программном обеспечении.
10. Сотрудники должны своевременно изменять пароли по умолчанию, используемые для процедур установки или сопровождения программного или компьютерного обеспечения.
11. Сотрудники должны изменять свои пароли после первого входа в систему при помощи пароля и после изменения пароля администратором.
12. Сотрудники должны пройти положительную идентификацию Сотрудника до того, как данному лицу будут представлены учетные данные для проверки подлинности.

    Процесс восстановления пароля должен включать средства положительной идентификации инициатора запроса перед предоставлением нового пароля.
13. Сотрудники не должны использовать механизмы сбора паролей или аутентификации личности Сотрудников, если только это не разрешено Руководством филиала компании PepsiCo и CISO.

    Персонал службы безопасности информационных технологий компании PepsiCo является исключением для данного стандарта.
14. Сотрудники должны использовать процессы аутентификации, контролируемые группой безопасности.
15. Сотрудники должны использовать процессы аутентификации, позволяющие разделение обеспечения безопасности и контроля деловых операций.
16. Сотрудники должны использовать процессы аутентификации, разработанные для предотвращения повторяющихся попыток несанкционированного доступа к учетным данным для проверки подлинности.

    Идентификатор может быть временно отключен после нескольких последовательных неверных запросов аутентификации пароля.

D. Стандарты по аутентификации для компании PepsiCo

1. Сообщения об ошибке аутентификации компании PepsiCo не должны содержать источник отказа.

   Примером является сообщение «неправильная регистрация», а не «неправильный пароль».
2. Пароли администратора компании PepsiCo должны изменяться сразу же после предполагаемого или известного несанкционированного доступа лица к системе или если Сотрудник, которому известен пароль, увольняется из компании PepsiCo.

3. Карманные компьютеры или коммуникаторы компании PepsiCo, оставленные без присмотра или бездействующие, должны отключаться или блокироваться экранной заставкой в течение периода времени, не превышающего 10 минут, и для возобновления работы необходимо введение пароля.

4. Сеансы аутентифицированных систем компании PepsiCo, оставленные без присмотра или бездействующие, должны выключаться или блокироваться в течение периода времени, не превышающего 10 минут.

E. Стандарты по управлению идентификационными данными:

1. Сотрудники должны своевременно проверять и вносить изменения в учетные данные для проверки подлинности при изменении рабочих обязанностей и своевременно отключать учетные данные для проверки подлинности, если Сотрудник прекращает деловое сотрудничество с компанией PepsiCo.
2. Руководство филиала компании PepsiCo предписывает прекращение использования любых учетных данных для проверки подлинности, если лицо, не являющееся сотрудником компании PepsiCo, становится ее сотрудником или если сотрудник компании PepsiCo перестает быть таковым. См. Часто задаваемые вопросы о переходе Сотрудников.
3. Сотрудники должны блокировать использование недействительных учетных данных для проверки подлинности через 90 дней.
4. Сотрудники должны удалять неиспользуемые учетные данные для проверки подлинности максимум через 400 дней.
5. Сотрудники должны хранить удостоверяющую информацию в соответствии с требованиями, приведенными в Политике управления документами компании PepsiCo.
6. Руководство филиала компании PepsiCo должно проверять учетные данные для проверки подлинности лица, не являющегося сотрудником компании PepsiCo, как минимум каждые 90 дней для лиц, имеющих доступ к информации, предназначенной для ограниченного пользования, и как минимум каждые 180 дней для лиц, имеющих доступ к информации, предназначенной только для внутреннего пользования.
7. Компания PepsiCo должна разрешать коллективное использование учетных данных системного администратора для проверки подлинности, если невозможно изменить учетные данные, включенные в программное или аппаратное обеспечение системы.

   Коллективное использование должно осуществляться минимальным количеством Сотрудников, необходимых для управления функциональными возможностями системы.
8. Сотрудники должны изменять пароль Сотрудника, использующего учетные данные системного администратора для проверки подлинности, если учетные данные данному лицу больше не нужны.
9. Руководство филиала компании PepsiCo должно хранить секретные учетные записи системного администратора для проверки подлинности.

   Учетные данные Администратора для проверки подлинности могут понадобиться в случае возникновения аварии. Примером секретной опции является абонентский ящик.
10. Сотрудники ведут учет предоставленных учетных данных для проверки подлинности.

    Данные записи должны включать Сотрудника, устройство или название процесса и контактную информацию, а не секретную часть учетных данных.
11. Сотрудники должны осуществлять разделение обязанностей по время управления идентификационными данными.

    Создатель и лицо, утверждающее учетные данные для проверки подлинности, должны быть разными лицами.

F. Авторизация

1. Сотрудники должны авторизоваться для получения информации, которая не является общедоступной.

   Действием по умолчанию является отказ в предоставлении доступа.
2. Сотрудники должны вести учет предоставленных прав доступа.

Данные записи должны включать Сотрудника, устройство или учетные данные для проверки подлинности процесса, а не секретную часть учетных данных.

3. Сотрудники должны осуществлять разделение обязанностей во время управления авторизацией.

   Лица, запрашивающие и утверждающие права доступа, должны быть разными лицами.

4. Владельцы информации или назначенное(-ые) лицо(-а) должно(-ы) проверять права доступа как минимум раз в год.

5. Владельцы информации или назначенное(-ые) лицо(-а) должно(-ы) проверять административные права доступа как минимум раз в 180 дней.

6. Системы компании PepsiCo должны использовать профили доступа (например, роли и группы) для предоставления доступа.

7. Системы компании PepsiCo должны отдавать предпочтение автоматизированным процессам и средствам управления.

   Целесообразные и применимые автоматизированные процессы и средства управления являются более эффективными, чем способы ручного управления при уменьшении количества ошибок.

8. Учетные данные администратора для проверки подлинности систем компании PepsiCo не должны иметь доступ к неадминистративным правам доступа.

9. Системы компании PepsiCo не должны документировать или отображать критические функции, которые Сотрудник не имеет права выполнять.

10. Системы компании PepsiCo должны полагаться на средства управления доступом к операционной системе, если операционная система или применимый пакет расширений управления доступом к операционной системе предоставляют данную услугу.

    При необходимости можно добавлять дополнительные средства управления доступом.

G. Доступ к записям

1. Процессы аутентификации компании PepsiCo должны как минимум регистрировать следующее:

   - Дата/время
   - Статус запроса
   - Идентификатор терминала/узла
   - Учетные данные Сотрудника для проверки подлинности

2. Административные процессы компании PepsiCo должны как минимум регистрировать следующие данные для каждого запроса на внесение дополнений/изменений:

   - Дата/время
   - Тип запроса
   - Статус запроса
   - Запрашиваемый доступ к функции/модулю
   - Учетные данные Сотрудника для проверки подлинности
   - Целевой объект внесения изменения (например, идентификатор или группа)

3. Сотрудники должны следить за точностью даты и времени систем, создающих записи в журналах.

H. Требования к управлению доступом к частной сети компании PepsiCo

1. Сотрудники должны делить частную сеть компании PepsiCo на подразделы при соответствующей степени региональной грануляции с учетом бизнес-требований и требований по защите информации.

   Каждый подраздел должен отделяться посредством пограничных устройств, предоставляющих санкционированный доступ и блокирующих любой иной доступ.

2. Сотрудники должны защищать компоненты сетевой инфраструктуры компании PepsiCo, такие как шлюзы, концентраторы, маршрутизаторы, выключатели и т.д. таким образом, чтобы административный и физический контроль ограничивался уполномоченным персоналом компании PepsiCo по проектированию и обслуживанию сетей.

3. Компания PepsiCo должна разрешать отключение или прерывание линий связи WAN или LAN для сохранения целостности сети при обнаружении несанкционированных изменений или неправильно установленного сетевого оборудования.
4. Частная сеть компании PepsiCo должна включать пограничные устройства, защищающие частную сеть компании PepsiCo и находящиеся под единоличным административным контролем компании PepsiCo при установлении соединения с сетями, не принадлежащими компании PepsiCo.
5. Пограничные устройства компании PepsiCo должны управляться согласно концепции «отказа по умолчанию» и настраиваться для блокировки всех доступов.

Специальные конфигурации должны использоваться в максимально ограниченном количестве сфер применения для предоставления разрешенного доступа.

6. Доступ за пределы границ сети компании PepsiCo никогда не должен превышать минимальное значение, необходимое для выполнения производственных функций.
7. Компания PepsiCo должна отказывать в доступе, запрашиваемом за пределами границ сети для выполнения определенной производственной функции, если открытие данного доступа может привести к возникновению неоправданной опасности для определенной производственной функции и (или) любой части сетевых и смежных систем компании PepsiCo.

7.3 Стандарт по предоставлению удаленного доступа

Настоящий *Стандарт по управлению удаленным доступом* основан на целях, приведенных в *Политике зашиты ресурсов*, и содержит специальные требования к соответствующим средствам управления идентификацией, аутентификацией (например, пароли) и авторизацией, необходимым для дистанционного доступа к информационным ресурсам компании PepsiCo.

7.3.1 Требования

A. Общие требования

1. Сотрудники должны использовать удаленный доступ к сети для утвержденных производственных необходимостей и выполнения установленных рабочих обязанностей.
2. Сотрудники должны соблюдать процесс запроса удаленного доступа к сети, утвержденный компанией PepsiCo.

   Процесс включает предоставление необходимых форм, содержащих описание информации и (или) систем, к которым необходим доступ, способы и сроки доступа, разрешение Владельца информации или назначенного лица и непосредственного начальника Сотрудника.
3. Сотрудники должны пройти техническую подготовку и подготовку по вопросам безопасности, утвержденные компанией PepsiCo, перед тем как получить удаленный доступ к сетям компании PepsiCo.
4. Сотрудники должны подключаться к сетям компании PepsiCo посредством правильно установленного и защищенного программного и аппаратного обеспечения, утвержденного компанией PepsiCo.
5. Удаленный доступ сторонних сотрудников к сети предусматривает поручительство сотрудника компании PepsiCo.

6. Компания PepsiCo не должна разрешать применение устройств с одновременным удаленным доступом к сети, подключенным к ее частной сети, если только это не разрешено Отделом проектирования сетей компании PepsiCo.

   Например, ПК не должен содержать модем, позволяющий устанавливать коммутируемое соединение, в то время как ПК подключен к частной сети компании PepsiCo.

B. Удаленный доступ

1. Компания PepsiCo должна требовать предоставления защиты своей информации в сетях и устройствах, не контролируемых компанией PepsiCo.
2. Компания PepsiCo должна предоставлять доступ к своей сети с сетей, не контролируемых компанией PepsiCo, только при наличии аутентификации на границе сети.
3. Сотрудники, аутентифицированные на границе сети, должны иметь те же права доступа, что и при непосредственном соединении с сетью, контролируемой компанией PepsiCo.

   При необходимости Владелец информации может использовать дополнительные ограничения доступа.
4. Беспроводные сетевые решения компании PepsiCo должны обеспечивать рост общего объема продаж или увеличение накоплений компании PepsiCo.
5. При необходимости Руководство филиала компании PepsiCo и CISO должны авторизовать беспроводные сетевые решения.
6. Руководство филиала компании PepsiCo должно разрабатывать процессы сбора данных об инвентаризации сети удаленного доступа и определять ненужные или самовольные установки для их удаления.
7. Руководство филиала компании PepsiCo должно определять основные процедуры обеспечения безопасности сети удаленного доступа, основанные на требованиях, приведенных в *Политике защиты ресурсов* и *Стандарте по оценке уязвимостей*.
8. Коммутирование телефонных номеров компании PepsiCo должно классифицироваться как информация, предназначенная только для внутреннего пользования, и защищаться соответствующим образом.
9. Сотрудники должны регулярно проверять журналы операций удаленного доступа для необычной или несанкционированной деятельности.
10. Компания PepsiCo должна рассматривать «туннели» (например, VPN), созданные посредством сетей, не контролируемых компанией PepsiCo, как часть частной сети компании PepsiCo, только если объекты, образующие конечные точки туннеля, соответствуют определению частной сети компании PepsiCo, а применение туннеля гарантирует, что логический канал передачи данных не доступен для сторон, кроме как компании PepsiCo.
11. Компания PepsiCo должна разрешать применение решений ограниченного удаленного доступа к сети для специальных подмножеств системы.

    Например, решение локальной беспроводной сети для портативных компьютеров может ограничивать использование беспроводного устройства для портативных компьютеров и сетевой доступ таким образом, что доступны только серверы, относящиеся к системам сбыта.

7.4 Стандарт по предоставлению физического доступа

Настоящий *Стандарт по предоставлению физического доступа* основан на целях, приведенных в *Политике защиты ресурсов*, и содержит специальные требования к соответствующим средствам управления физическим доступом к информационным ресурсам компании PepsiCo.

7.4.1 Требования

A. Общие требования

1. Сотрудники должны предоставлять средства управления доступом к следующим видам объектов информационных технологий:

   ■ Центр обработки и передачи данных
   ■ Серверное помещение
   ■ Печатный центр
   ■ Телекоммуникационное помещение
   ■ Лаборатории по разработке систем, технические лаборатории или лаборатории обеспечения качества
   ■ Точка телекоммуникационного доступа или иные объекты информационных технологий
   ■ Иные объекты информационных технологий, считаемые необходимыми.

2. Сотрудники не должны указывать объекты информационных технологий компании PepsiCo способом, который привлечет нежелательное внимание к объектам или приведет к разглашению его назначения.

3. Сотрудники должны устанавливать и обслуживать дверные замки.

4. Сотрудники должны применять и обслуживать соответствующие средства управления доступом для ограничения, контроля и отслеживания доступа к объектам информационных технологий.

5. Сотрудники должны регулярно проверять средства управления физическим доступом.

6. Сотрудники, которые проводят в центре обработки и передачи данных 75 % своего времени, должны иметь постоянный локальный доступ.

7. Сотрудники не должны перемещать или снимать оборудование с объектов информационных технологий компании PepsiCo без разрешения.

8. Сотрудники должны незамедлительно передать управление ресурсами компании PepsiCo, если они прекратили деловое сотрудничество с компанией PepsiCo или при изменении предписанных рабочих обязанностей, для которых больше не нужен доступ к объектам.

   Ресурсы компании PepsiCo могут включать оборудование, карты доступа, ключи, комбинации цифр кодового замка, пароли и иные устройства управления доступом. При необходимости они должны своевременно изменяться.

9. Компания PepsiCo должна требовать, чтобы объекты информационных технологий, являющиеся внешними для помещений компании PepsiCo, соответствовали требованиям данного *Стандарта по предоставлению физического доступа*.

   Примеры внешних помещений включают совместно размещенные объекты, абстрактные сервисные примитивы и объекты сторонних поставщиков.

B. Центры обработки и передачи данных и иные основные объекты информационных технологий

1. Сотрудники должны соблюдать Стандарты, приведенные в разделе требований *Стандарта по предоставлению физического доступа*.

2. Сотрудники должны устанавливать и обслуживать автоматически закрывающиеся двери с сигнализацией, которая активируется, если двери остаются открытыми дольше заданного периода времени.
3. Сотрудники должны иметь возможность видеть и устно общаться из помещения с теми, кто находится у наружного входа.
4. Сотрудники должны дополнять системы управления доступом при аутентификации (например, магнитный бедж или доступ по карточкам) средствами физического контроля (например, дверные замки).
5. Сотрудники должны регистрировать доступ к объектам информационных технологий в журнале.
6. Сотрудники должны регистрировать посетителей компании PepsiCo в журнале отдельно от регулярной регистрации операционным доступом.
7. Посетители компании PepsiCo должны носить утвержденный бедж для идентификации посетителя на видном месте и постоянно сопровождаться.

C. Материально-техническая база и персонал

1. Сотрудники должны устанавливать регулируемые системы вентиляции, отопления, кондиционирования воздуха и инженерные сети, соответствующие:

   ■ Требованиям к доступности бизнес-систем
   ■ Производственным требованиям к обслуживанию инфраструктуры информационных технологий
   ■ Эксплуатационным характеристикам оборудования информационных технологий, установленного на объекте
2. Сотрудники не должны курить, есть или пить в помещениях, где находятся технические средства.
3. При необходимости Сотрудники должны устанавливать средства обнаружения и предотвращения пожаров, такие как огнетушители и дымовые извещатели.
4. Сотрудники должны организовывать объекты и оборудование компании PepsiCo.

   Объекты не должны содержать бумагу, коробку, иные возможные горючие нагрузки и экологические опасности для снижения риска возникновения несчастного случая.
5. Сотрудники должны четко организовывать кабели, соединяющие компьютер и вспомогательное оборудование, и следить за тем, чтобы они не загромождали проходы.
6. Сотрудники должны применять структурированные системы для электропроводки и проводки кабельных сетей.

D. Физическая информационная безопасность Сотрудника

1. Сотрудники должны обеспечивать безопасность ключей от столов, картотек, компьютеров и дверей офисов.
2. Сотрудники должны обеспечивать безопасность объектов, где обрабатывается и хранится информация, предназначенная только для внутреннего и для ограниченного пользования.
3. Сотрудники должны обеспечивать защиту всех съемных носителей и печатных копий информации, предназначенной только для внутреннего и для ограниченного пользования, если она не используется.
4. Сотрудники должны размещать свои компьютеры таким образом, чтобы клавиатуры и экраны не просматривались из проходов, дверных проемов и окон, на основании уровня секретности обрабатываемой информации и общей безопасности объекта.
5. Сотрудники должны размещать принтеры, ксероксы и факсы в безопасном месте на основании уровня секретности выходных данных.

7.5 Стандарт шифрования

Настоящий *Стандарт шифрования* основан на целях, приведенных в *Политике защиты ресурсов*, и содержит специальные требования к шифрованию конфиденциальных информационных ресурсов компании PepsiCo.

7.5.1 Требования

A. Общие требования

1. Сотрудники должны использовать шифрование в соответствии с действующим законодательством и нормами.
2. Сотрудники не должны использовать технологии шифрования в случае информации, предназначенной для ограниченного пользования, если только это не разрешено Руководством филиала компании PepsiCo и CISO.
3. Сотрудники должны создавать и защищать ключи шифрования компании PepsiCo в соответствии с требованиями, приведенными в *Стандарте по управлению доступом*, для информации, предназначенной для ограниченного пользования.
4. Сотрудники должны сразу же сообщать о скомпрометированных ключах шифрования в Центр технической поддержки компании PepsiCo или местный центр поддержки.

B. Алгоритмы предоставления сообщения в краткой форме

1. Алгоритмы предоставления сообщения в краткой форме компании PepsiCo приведены ниже:
   - MD5
   - SHA-1 с 128-битным или 160-битным ключом
2. Сотрудники должны использовать MD5 только для хеширования файлов.
3. Сотрудники не должны использовать MD5 в подписях и сертификатах.

C. Алгоритмы симметричного шифрования

1. Алгоритмы симметричного блочного шифрования, утвержденные компанией PepsiCo, приведены ниже:
   - Blowfish
   - Triple-DES
   - Программа защиты сообщений (PGP)
   - Уровень защищенных сокетов (SSL)
   - Расширенный стандарт шифрования (AES)
2. Сотрудники должны предоставлять ключи шифрования в централизованное хранилище до начала шифрования посредством любого алгоритма симметричного шифрования, утвержденного компанией PepsiCo.

   Данное действие обеспечивает возможность получения информации компанией PepsiCo.
3. Сотрудники должны создавать и защищать симметричные ключи компании PepsiCo в соответствии с требованиями, приведенными в *Стандарте по управлению доступом*, для информации, предназначенной для ограниченного пользования.

D. Алгоритмы ассиметричного шифрования

1. Алгоритмы ассиметричного шифрования, утвержденные компанией PepsiCo, приведены ниже:
   - Алгоритм Ривеста-Шамира-Эдльмана с максимально возможной стойкостью бита ключа
   - Алгоритм Диффи-Хеллмана с максимально возможной стойкостью бита ключа
2. Сотрудники должны использовать ключи подписи или дополнительные ключи расшифровки компании PepsiCo с пакетами программ шифрования с открытым ключом.
   Данное действие обеспечивает возможность получения информации компанией PepsiCo.

3. Сотрудники должны избавляться от временных сеансовых ключей депонирования, используемых криптосистемами с открытыми ключами, такими как Виртуальные частные сети (VPN).

4. Сотрудники должны создавать и защищать открытые ключи компании PepsiCo в соответствии с требованиями, приведенными в *Стандарте по управлению доступом*, для информации, предназначенной для ограниченного пользования.

7.6 Стандарт по защите от угроз доступности информации

Настоящий *Стандарт по защите от угроз доступности информации* основан на целях, приведенных в *Политике защиты ресурсов*, и содержит специальные требования к защите доступности информационных ресурсов компании PepsiCo.

7.6.1 Требования

A. Общие требования

1. Сотрудники должны использовать средства управления при проектировании процессов таким образом, чтобы информационные ресурсы были постоянно доступны для обеспечения выполнения производственных операций.

2. Сотрудники должны сразу же сообщать об отказах системы или сети в Центр технической поддержки компании PepsiCo или местный центр поддержки.

3. Сотрудники должны направлять предварительное уведомление о плановых простоях (например, техническое обслуживание системы) тем, кого затрагивают изменения в работе.

4. Сотрудники должны составлять Отчет о последствиях для безопасности и Анализ последствий для деятельности перед утверждением внедрения новых или модифицированных бизнес-систем.

5. Сотрудники должны использовать методы управления емкостью и распределения нагрузки для минимизации рисков и последствий отказов систем.

B. Резервирование данных

1. Сотрудники должны планировать и регистрировать расписания резервного копирования.

2. Владельцы информации или назначенное(-ые) лицо(-а) должно(-ы) утверждать расписания резервного копирования.

3. Сотрудники должны планировать и осуществлять резервное копирование во время минимального воздействия на систему и в логической точке восстановления.

4. Сотрудники должны помечать, собирать и трассировать копируемую информацию.

5. Сотрудники должны обрабатывать информацию, заархивированную для резервного копирования, способом, соответствующим уровню секретности исходной информации в соответствии с требованиями, приведенными в *Стандарте по обозначению и обращению с информацией*.

   Если объединяется информация, относящаяся к разным уровням секретности, то итоговая совокупность информации или новая информация классифицируется по наиболее ограничивающему уровню источников.

6. Сотрудники должны регулярно проверять резервные копии для подтверждения возможности восстановления данных.

7. Сотрудники должны хранить резервные копии в соответствии с требованиями, приведенными в Политике управления документами компании PepsiCo.

C. Дублирование и восстановление после отказа

1. Сотрудники должны использовать аппаратное резервирование для оборудования, поддерживающего службы и системы для решения критически важных задач.

   Примерами оборудования являются серверы и элементы сетевой инфраструктуры.

2. Сотрудники должны иметь запчасти к критическим базовым компонентам, таким как маршрутизаторы и коммутаторы, и средства обслуживания должны предусматривать своевременную замену деталей.

3. Сотрудники должны оценивать каждое сетевое подключение для определения последствий простоя для деятельности и обеспечивать наличие резервных линий связи или обходной маршрутизации для критических соединений.

4. Сотрудники не должны базировать сетевые подключения на коллективном пользовании Интернетом для систем, если простой приведет к существенным неблагоприятным последствиям для деятельности.

   Например, не допускаются подключения, критические для деятельности, в VPN с регулярной структурой.

D. Планы послеаварийного восстановления (DR) и устойчивости функционирования (BCP)

1. Сотрудники должны сверяться с руководящими документами по послеаварийному восстановлению и устойчивости функционирования компании PepsiCo.

7.7 Стандарт по антивирусной защите

Настоящий *Стандарт по антивирусной защите* основан на целях, приведенных в *Политике защиты ресурсов*, и содержит специальные требования к защите информационных ресурсов компании PepsiCo от вирусов и иных вредоносных кодов.

7.7.1 Требования

A. Общие требования

1. Сотрудники не должны отключать, изменять или обходить корпоративную антивирусную защиту систем компании PepsiCo.

2. Сотрудники должны использовать антивирусное экранирующее программное обеспечение в межсетевых защитных экранах, серверах, шлюзах и офисных компьютерах (например, настольные, портативные и переносные компьютеры).

3. Сотрудники должны своевременно обновлять антивирусное программное обеспечение и базы.

4. Сотрудники не должны преднамеренно записывать, создавать, компилировать, копировать, собирать, распространять, выполнять или пытаться вводить любой вирус или код компьютера, разработанный для повреждения вычислительной среды компании PepsiCo.

5. Сотрудники должны выполнять соответствующие антивирусные процедуры, если известно или предполагается наличие компьютерного вируса в любом вычислительном или коммуникационном устройстве.

   Обычно обнаруженные заражения вирусом автоматически «очищаются». Если данная характеристика недоступна, все файлы, программы и системы, зараженные вирусом, должны изолироваться и помещаться в карантин до удаления.

6. Сотрудники должны сразу же сообщать о наличии вируса в вычислительном или коммуникационном устройстве в Центр технической поддержки компании PepsiCo или местный центр поддержки, если вирус присутствует после проведения необходимой антивирусной процедуры.

7. Сотрудники должны убедиться в отсутствии вирусов в программном обеспечении и на съемных носителях перед их использованием в компьютерной среде компании PepsiCo.
8. Сотрудники должны изменять имя пользователя и загрузочные сценарии для запуска антивирусного программного обеспечения, утвержденного компанией PepsiCo, которое проверяет память системы и загрузочные секторы на наличие вирусов и иных вредоносных кодов.
9. Сотрудники должны вести, проверять и хранить журналы сканирования вирусов в соответствии с требованиями, приведенными в *Стандарте по аудиту*.

B. Клиенты

1. Сотрудники должны еженедельно проводить полное сканирование всех сетевых локальных дисков.

2. Сотрудники должны отправлять предупреждающее сообщение отправителю электронного сообщения, если электронное сообщение заражено вирусом.
Сотрудники не должны пересылать или отвечать на зараженное электронное сообщение.

C. Серверы

1. Сотрудники должны устанавливать и запускать антивирусное программное обеспечение на серверах, которые сканируют все входящие данные, и регулярно проводить полное сканирование вирусов всех томов хранилища.
2. Сотрудники должны ежедневно осуществлять сканирование сетевых локальных дисков и томов в режиме обнаружения вирусов во время низкого использования.

   Сканирование не должно конфликтовать или мешать иным регламентным системным или оперативным операциям (например, резервному копированию и производственным пакетным заданиям).

D. Демилитаризованная зона

1. Сотрудники должны использовать антивирусное программное обеспечение для остановки распространения вирусов и иных вредоносных кодов по сети периметра перед тем, как они попадут в сеть компании PepsiCo.
2. Сотрудники должны сканировать и определять отсутствие вирусов в любых электронных сообщениях, приложениях и сжатых файлах перед их прохождением через межсетевые защитные экраны (файерволы) и сеть периметра компании PepsiCo.

7.8 Стандарт по аудиту

Настоящий *Стандарт по аудиту* основан на целях, приведенных в *Политике защиты ресурсов*, и содержит специальные требования к проведению аудита и регистрации информационных ресурсов компании PepsiCo, включая активацию, защиту и хранение.

7.8.1 Требования

A. Общие требования

1. Сотрудники должны применять централизованную схему ведения контрольных журналов для безопасного хранения журналов аудита.
2. Сотрудники, обладающие специальными полномочиями, должны проверять журналы аудита для обнаружения данных, связанных со злоумышленной деятельностью, и принятия соответствующих мер согласно *Стандарту по контролю угроз* и *Стандарту по реагированию на инциденты*.

3. Серверы, сетевые устройства и многопользовательские системы компании PepsiCo должны получать синхронизацию времени из определенного и стандартизированного источника времени.

B. Запуск

1. Сотрудники должны проводить аудит серверов, сетевых устройств и многопользовательских систем в установленном порядке.
2. Сотрудники должны регистрировать изменения в безопасности, критические функции и функции с высокой степенью риска. Иные действия по ведению журнала включают следующее:

   ■ активность пользователя (например, неудачные попытки входа в систему)
   ■ работа системы (например, непредвиденные перезагрузки)
   ■ сетевые подключения (например, подключения в необычное время)
   ■ контроль сетевого трафика (например, развертывания пространства сетевых адресов)
   ■ работа программно-зависимого журнала регистрации (например, избыточное или необычное количество операций передачи файлов)

3. Аудиторская документация компании PepsiCo должна включать с кем, с чем, когда и откуда возникло зарегистрированное событие или действие.

C. Защита

1. Сотрудники должны защищать журналы аудита и записи от несанкционированного вмешательства (например, удаления или изменения).
2. Сотрудники должны ограничивать доступ привилегированных учетных записей к журналам аудита, аудиторской документации и аудиторских конфигураций.

D. Хранение

1. Сотрудники должны сохранять журналы аудита на альтернативный носитель до реинициализации.
2. Сотрудники должны следить за тем, чтобы объем памяти был достаточен для предотвращения перезаписи журналов регистрации.
3. Сотрудники должны хранить журналы аудита не менее 30 дней.
4. Сотрудники должны архивировать журналы аудита, относящиеся к безопасности, на носителях с защитой от записи и хранить их в соответствии с требованиями, приведенными в *Политике управления документами* компании PepsiCo и действующем законодательстве и нормах.

8 Управление ресурсами

8.1 Политика управления ресурсами

8.1.1 Программное заявление

Настоящая *Политика управления ресурсами* определяет цели компании PepsiCo по созданию специальных стандартов по управлению сетями и системами, обрабатывающими, передающими и хранящими информационные ресурсы компании PepsiCo.

8.1.2 Цели

ИТ-системы компании PepsiCo, включая аппаратное и программное обеспечение, должны управляться в соответствии с целями, приведенными в *Политике защиты ресурсов,* в течение всего жизненного цикла (т.е. с момента приобретения до утилизации). Методика разработки программного обеспечения жизненного цикла (SDLC) представляет стандартный пошаговый процесс создания и внедрения компьютерной системы. С другой стороны, управление жизненным циклом относится к требованиям по управлению жизненным циклом средств обеспечения информационной безопасности. Специальные требования к управлению жизненным циклом приведены в *Стандарте по управлению жизненным циклом*.

Компания PepsiCo создает и придерживается основных стандартов защиты в соответствии с целями, приведенными в *Политике защиты ресурсов,* для каждой системы, представленной в производственной среде компании PepsiCo. Конфигурация производственных систем и инфраструктура информационных технологий должны контролироваться во избежание возможности ослабления безопасности системы, доступности или производительности. Специальные требования к управлению конфигурациями приведены в *Стандарте по управлению конфигурациями*.

Системы и сети, используемые в производственной среде компании PepsiCo, должны придерживаться утвержденных процессов и процедур управления изменениями для обеспечения внесения только санкционированных обновлений и изменений. Специальные требования к управлению изменениями приведены в *Стандарте по управлению изменениями*.

Системы и сети, разработанные компанией PepsiCo или от ее имени, должны придерживаться утвержденных процессов для анализа, разработки, проектирования, проверки и улучшения систем и сетей для обеспечения объединения соответствующих средств управления безопасностью. Специальные требования к проектированию систем не приведены в настоящем документе, но могут выполняться посредством применения любой методики разработки программного обеспечения жизненного цикла, утвержденной компанией PepsiCo.

8.1.3 Обязанности

Руководство филиала компании PepsiCo несет ответственность за доведение до сведения и рассмотрение в своих организационных подразделениях *Политики управления активами* и смежных стандартов. Руководство филиала компании PepsiCo также несет ответственность за определение, утверждение и выполнение процедур по обеспечению соблюдения политики и стандартов.

Сотрудники несут ответственность за изучение и соблюдение *Политики управления активами* и смежных стандартов.

8.2 Стандарт по управлению жизненным циклом

Настоящий *Стандарт по управлению жизненным циклом* основан на целях, приведенных в *Политике управления ресурсами*, и содержит специальные требования к управлению жизненным циклом информационных систем компании PepsiCo, включая аппаратное и программное обеспечение.

8.2.1 Требования

A. Фаза проектирования/закупки

1. Оценки рисков компании PepsiCo должны включать:

   ■ Проверку соблюдения нормативных требований
   ■ Область применения, соответствующую уровню секретности, критичности, сложности и стоимости системы
   ■ Проверку информационных ресурсов, угроз и уязвимостей системы для решения критически важных задач для определения наиболее эффективных средств управления безопасностью

2. Требования компании PepsiCo к безопасности должны включать:

   ■ Проектную документацию архитектуры системы безопасности, которая относится к:
      ✓ Потокам данных
      ✓ Техническим средствам управления безопасностью на уровне приложения, базы данных, сервера и сети
      ✓ Периодической проверке средств управления безопасностью на каждом этапе разработки программного обеспечения жизненного цикла (SDLC), утвержденном компанией PepsiCo
   ■ Существующие средства управления безопасностью
   ■ Возможность проверять журналы, генерируемые системой
   ■ Поддержку функциональных потребностей системы
   ■ Возможность регистрировать действия по управлению безопасностью
   ■ Защиту от удаления или изменения аудиторской документации и журналов аудита
   ■ Функции управления безопасностью и вспомогательные ресурсы, необходимые для технического обслуживания
   ■ Поддержку при распределении функциональных возможностей между доступом Сотрудника и администратора
   ■ Соблюдение действующих корпоративных политик и стандартов, законов и норм
   ■ Требования к подбору персонала для выполнения текущих функций управления безопасностью

3. Договорные требования компании PepsiCo должны включать:

   ■ Требования к обеспечению безопасности при закупке аппаратного и программного обеспечения
   ■ Положения по защите конфиденциальной информации компании PepsiCo (например, конфигурация системы и параметры безопасности) поставщиком услуг, оказывающим техническую поддержку

B. Фаза реализации

1. Требования компании PepsiCo к реализации должны включать:

   ■ Подготовку администраторов службы безопасности относительно новых обязанностей по обеспечению безопасности
   ■ Средства управления безопасностью, надлежащим образом настроенные и включенные перед началом производства системы
   ■ Процедуры обеспечения управления безопасностью на двух системах во время реализации, если новая система заменяет существующую

2. Требования компании PepsiCo к проведению испытаний должны включать:

   ■ Проверку функций управления безопасностью
   ■ Проверку безопасности систем для решения критически важных задач для определения соответствия требованиям к обеспечению безопасности

3. Требования обеспечения документацией компании PepsiCo должны включать:

   ■ Соответствующую документацию поставщика услуг по обеспечению безопасности для закупленного аппаратного и программного обеспечения

■ Письменную сертификацию средств управления безопасностью для программного обеспечения для решения критически важных задач, разработанного поставщиком услуг
■ Распространение учебных материалов по функциональным возможностям обеспечения безопасности среди уполномоченного персонала

C. Фаза эксплуатации/сопровождения

1. Требования компании PepsiCo к мерам безопасности и управлению безопасностью должны включать:

■ Задачи и действия по обеспечению безопасности, которые регулярно (включая, помимо прочего):
✓ Осуществляют резервное копирование
✓ Управляют доступом Сотрудников
✓ Проводят обучение и подготовку новых администраторов
✓ Проводят регулярную оценку уязвимостей системы и рисков
✓ Проверяют и контролируют в соответствии с требованиями, приведенными в *Стандарте по контролю угроз*
✓ Осуществляют техническое обслуживание системы безопасности (т.е. проверку и применение обновлений и исправления для системы безопасности)
■ Соответствующее резервное копирование и удаление конфиденциальной информации перед отправкой компонентов системы за пределы площадки для проведения технического обслуживания

2. Требования компании PepsiCo к управлению изменениями должны включать:

■ Внесение изменений в операционные системы производственной среды компании PepsiCo в соответствии со *Стандартом по управлению изменениями*

3. Требования компании PepsiCo к защите вычислительных устройств должны включать:

■ Своевременное сообщение о краже или потере вычислительных устройств компании PepsiCo
■ Сертификацию восстановленных вычислительных устройств после потери перед подключением к сети компании PepsiCo
■ Разумные меры предосторожности, предпринимаемые Сотрудниками относительно кражи, потери или повреждения любого вычислительного устройства компании PepsiCo

D. Фаза использования

1. Требования компании PepsiCo к безопасному использованию должны включать:

■ Соблюдение действующих лицензионных соглашений по использованию программного обеспечения.
■ Уничтожение физического носителя, содержащего информацию, предназначенную только для внутреннего или для ограниченного пользования.
■ Соблюдение действующих корпоративных политик и стандартов, законов и норм относительно требований к хранению системных данных.
■ Проверку конфиденциальной информации перед использованием для определения, следует ли ее передавать, архивировать, отбросить или уничтожить.
■ Соблюдение действующих корпоративных политик и стандартов, законов, норм и положений об окружающей среде для использования системных компонентов, таких как аппаратное и программное обеспечение.
■ Удаление или безопасное перезаписывание информации, предназначенной только для внутреннего или для ограниченного пользования, с вычислительных или коммуникационных устройств до начала использования (например, передача, отбрасывание или возврат).

8.3 Стандарт по управлению конфигурациями

Настоящий *Стандарт по управлению конфигурациями* основан на целях, приведенных в *Политике управления ресурсами*, и содержит специальные требования к защите сетей, серверов, баз данных, настольных компьютеров и иных вычислительных устройств компании PepsiCo.

8.3.1 Требования

A. Общие требования

1. Сотрудники должны проверять последствия нарушения безопасности путем внесения изменений в системы и инфраструктуру информационных технологий.
2. Процессы управления конфигурациями компании PepsiCo должны содержать конфигурационные данные до и после внесения изменения.
3. Сотрудники должны проявлять должную заботливость при применении обновлений для системы безопасности (например, патчей для устранения ошибок защиты и обновленных версий).
4. Сотрудники должны подтверждать развертывание системы для соответствия указанным техническим требованиям до начала реализации.
5. Сотрудники должны регулярно проверять системы для определения и удаления ненужных сервисов.
6. Сотрудники должны создавать резервные копии основных экземпляров конфигурации для систем в соответствии со *Стандартом по защите от угроз доступности информации*.

B. Рабочие сетевые устройства

1. Сотрудники должны настраивать сетевые устройства в соответствии с утвержденными техническими требованиями к конфигурации.
2. Сотрудники должны идентифицировать сетевые устройства следующим образом:
   - Физическое местоположение
   - Версия операционной системы (или эквивалента)
   - Проверка версий операционной системы (или эквивалента) и исправлений
   - Параметры безопасности и конфигурации аппаратного и программного обеспечения
3. Сотрудники должны управлять и обслуживать сетевые устройства для выполнения целей компании PepsiCo по контролю угроз в соответствии со *Стандартом по контролю угроз* и *Стандартом по реагированию на инциденты*.

C. Рабочие серверы

1. Сотрудники должны настраивать серверы в соответствии с утвержденными техническими требованиями к конфигурации.
2. Сотрудники должны идентифицировать серверы следующим образом:
   - Периферийные устройства
   - Физическое местоположение
   - Версии микропрограммного обеспечения
   - Версия операционной системы (или эквивалента)
   - Проверка версий операционной системы (или эквивалента) и исправлений
   - Параметры безопасности и конфигурации аппаратного и программного обеспечения
3. Сотрудники должны обеспечивать соответствие конфигураций сервера требованиям, приведенным в *Политике защиты ресурсов*.
4. Сотрудники должны управлять и обслуживать серверы для выполнения целей компании PepsiCo по контролю угроз в соответствии со *Стандартом по контролю угроз* и *Стандартом по реагированию на инциденты*.

D. Рабочие базы данных

1. Сотрудники должны настраивать базу данных в соответствии с утвержденными техническими требованиями к конфигурации.

2. Сотрудники должны идентифицировать базы данных следующим образом:

   - Периферийные устройства
   - Физическое местоположение
   - Версии микропрограммного обеспечения
   - Версия операционной системы (или эквивалента)
   - Проверка версий операционной системы (или эквивалента) и исправлений
   - Параметры безопасности и конфигурации аппаратного и программного обеспечения

E. Рабочая настольная среда

1. Сотрудники должны настраивать настольные компьютеры в соответствии с утвержденными техническими требованиями к конфигурации.
2. Сотрудники не должны устанавливать несанкционированное аппаратное или программное обеспечение на настольных или портативных компьютерах.
3. Сотрудники должны распространять стандартное программное обеспечение, обновления и корректировки электронным образом и использовать соответствующие метрические значения для определения коэффициентов выполнения нагрузок и соблюдения требований, приведенных в *Правилах допустимого использования* и *Стандарте по управлению уязвимостями*.
4. Сотрудники должны проводить плановые и (или) необъявленные проверки аппаратного и программного обеспечения на настольных и портативных системах для обнаружения и удаления компонентов, не соответствующих требованиям компании PepsiCo.

8.4 Стандарт по управлению изменениями

Настоящий *Стандарт по управлению изменениями* основан на целях, приведенных в *Политике управления ресурсами*, и содержит специальные требования к следующим утвержденным процессам и процедурам при внесении изменений в системы и сети в производственной среде компании PepsiCo.

8.4.1 Требования

A. Общие требования

1. Сотрудники, уполномоченные вносить изменения, должны соблюдать процесс управления изменениями, утвержденный компанией PepsiCo.
2. При необходимости Сотрудники должны отображать существенные изменения в планах устойчивости функционирования и (или) послеаварийного восстановления.
3. Сотрудники должны проводить анализ последствий для безопасности до внесения изменений.

B. Запрос на внесение изменений

1. Сотрудники должны использовать процедуры и средства, утвержденные компанией PepsiCo, для своевременного предоставления запросов на внесение изменений и сопроводительной документации уполномоченному утверждающему лицу (например, Консультативный совет по внесению изменений – CAB) (например, за две недели до проведения следующего запланированного собрания по управлению изменениями для утверждения CAB).
2. Запросы компании PepsiCo на внесение изменений должны содержать следующую информацию:

   - Очередность
   - Дата подачи
   - Дата запроса на внесение изменений
   - Описание изменения
   - Обоснование внесения изменения

- При необходимости обоснование затрат
- Последствия для производственной среды
- Имя и контактные данные инициатора запроса

3. Запросы на внесение изменений компании PepsiCo должны относиться к одной из четырех следующих категорий очередности:

Очередность	Описание	Срок реализации
Критический	Серьезные последствия для деятельности и производства, если не реализовать сразу же. Обязательно и должно реализовываться.	Реализуется в течение 10 рабочих дней после утверждения.
Высокий	Существенные последствия для деятельности и производства, если не реализуется. Существенное и (или) незамедлительное улучшение производственной среды. Относится к неотложным вопросам нормативно-правового регулирования конкурентного рынка.	Реализуется в течение 30 рабочих дней после утверждения.
Средний	Умеренные последствия для деятельности и производства, если не реализуется. Умеренное улучшение производственной среды.	Реализуется в течение 60 рабочих дней после утверждения.
Низкий	Относится к отсутствию последствий для деятельности и производства, если не реализуется. Незначительное улучшение производственной среды.	Реализуется не ранее 90 рабочих дней после утверждения.

C. Проверка и оценка вносимых изменений

1. Процесс проверки и оценки вносимых изменений компании PepsiCo должен включать как минимум следующее:

- Подтверждение всех представленных запросов на внесение изменений
- Определение и доведение до сведения сроков проведения проверки для всех представленных запросов на внесение изменений
- Проверка запросов и сопроводительной документации квалифицированными сотрудниками, представляющими системы и (или) производственные функции, на которые изменения оказывают воздействие

D. Утверждение изменения

1. Процесс утверждения изменения компании PepsiCo должен включать как минимум следующее:

- Рекомендации по утверждению, отклонению или отсрочке рассмотренных запросов на внесение изменений
- Пояснения по всем отклоненным или отсроченным запросам на внесение изменений
- Внесение утвержденных запросов на внесение изменений в специальные графики текущего технического обслуживания.

2. Сотрудники могут подавать апелляцию, если запрос на внесение изменений не утвержден.

E. Проведение испытаний

1. Компания PepsiCo должна использовать среду технологической подготовки, отдельно от проектной и производственной среды, для испытания внесенных изменений до их реализации.
2. Компания PepsiCo должна оценивать риски нарушения безопасности и защищать конфиденциальность, доступность и целостность информационных ресурсов промышленных систем во время проведения испытаний.
3. Сотрудники должны вносить изменения в программное обеспечение в проектной среде и при необходимости передавать их в среду технологической подготовки.

F. Документация

1. Сотрудники должны согласовывать следующую сопроводительную документацию до начала реализации утвержденных изменений в производственной среде:
   - Выполнение задач по составлению контрольных списков и оценок продолжительности
   - Последовательное начало выполнения процедур, обязательств и действий
   - Процедуры отмены и действия по восстановлению
   - Процедуры проведения испытаний для подтверждения изменений

G. Реализация

1. Сотрудники не должны предоставлять разработчикам независимый доступ для передачи исходного кода в производственную среду.
2. Сотрудники должны разрешать ограниченному количеству лиц передавать программное обеспечение из среды технологической подготовки в производственную среду.
3. Сотрудники, уполномоченные компанией PepsiCo реализовывать утвержденные изменения, должны соблюдать процедуры развертывания, зафиксированные и утвержденные компанией PepsiCo.

H. Подтверждение и отслеживание

1. Сотрудники должны подтверждать реализацию изменений для гарантии отсутствия уязвимостей в системе и (или) приостановления оказания услуг.
2. Сотрудники, уполномоченные Руководством филиала компании PepsiCo, должны соблюдать установленные процедуры отмены для возврата производственной среды в состояние до реализации изменения, если в результате реализации изменений в системе возникли уязвимости и (или) оказание услуг было приостановлено.
3. При необходимости Сотрудники, не зависящие от перемещений изменений, должны сообщать о результатах внесения изменений Владельцу(-ам) информации или назначенному(-ым) Менеджеру(-ам) по управлению изменениями.
4. При необходимости Сотрудники должны обновлять основную документацию по конфигурации, текущую версию программы и сценарии, если внесенные изменения приняты в качестве производственных норм.

I. Аварийные изменения

1. При необходимости компания PepsiCo должна требовать от Владельца информации и Руководителя филиала компании PepsiCo или соответствующих назначенных лиц утверждения аварийных изменений.

   При участии Консультативного совета по внесению изменений (CAB) представитель данного совета также должен утверждать изменение.
2. Сотрудники должны предоставлять соответствующий доступ лицам для устранения актуальных ошибок в программном обеспечении или решения производственных вопросов во время выполнения чрезвычайных процедур.
3. Сотрудники должны контролировать и регистрировать действия при необходимости предоставления специального доступа к производственным ресурсам.

4. Сотрудники должны аннулировать специальный индивидуальный доступ к производственным ресурсам сразу после реализации аварийных изменений.
5. При необходимости Сотрудники, не зависящие от перемещений изменений в производстве, должны сообщать о причинах внесения аварийных изменений, действиях, предпринимаемых для устранения проблем, и результатах внесения изменений Владельцу(-ам) информации или назначенному(-ым) Менеджеру(-ам) по управлению изменениями.

   При участии Консультативного совета по внесению изменений (CAB) эта же информация предоставляется и совету.

9 Глоссарий

ТЕРМИН	ОПРЕДЕЛЕНИЕ
Сотрудник	Служащие, подрядчики, временные работники и работники, занятые неполный день, а также те, кто привлекается иными лицами для выполнения работы в помещениях компании PepsiCo или имеет доступ к информации, системам, компьютерам, сетям, телекоммуникациям и передачи сообщений и иным информационным службам компании PepsiCo. См. развернутое определение в Разделе 1.3 настоящего документа.
Аутентификация	Процесс, идентифицирующий или подтверждающий приемлемость рабочей станции, инициатора или Сотрудника для получения доступа к специальным категориям информации. Аутентификация обеспечивает гарантию относительно идентифицируемости субъекта или объекта.
План устойчивости функционирования (BCP)	Реализация альтернативных производственных процессов и процедур, которые обходят системные области, находящиеся под воздействием аварии. Данный возврат к ручной системе позволяет бизнес-направлениям функционировать во время восстановления технологий и технических компонентов и данных.
CISO	Руководитель по информационной безопасности. Сотрудник компании PepsiCo, несущий ответственность за глобальное управление информационной безопасностью и ответственный за смягчение последствий технических, деловых и правовых рисков для предприятия. CISO составляет Концепцию программы обеспечения информационной безопасности компании PepsiCo и управляет программой в соответствии с целями и концепциями.
Управление конфигурациями (CM)	Метод перечисления и хранения подробных данных обо всем аппаратном обеспечении (например, местоположение и сетевой адрес) и программном обеспечении (например, текущая версия и применяемые обновления) с целью предоставления технической информации для обнаружения и устранения неисправностей и дальнейшего обновления.
Послеаварийное восстановление (DR)	Восстановление технических платформ, технических компонентов, инфраструктуры, приложений и данных в альтернативном центре обработки данных после крупной аварии или отказа в основном месте центра обработки данных.
Шифрование	Кодирование данных для достижения целей обеспечения конфиденциальности, анонимности, отметки времени и иных целей безопасности.
Межсетевой защитный экран	Система или сочетание систем, устанавливающая границу между двумя или несколькими сетями.

ТЕРМИН	ОПРЕДЕЛЕНИЕ
Информация	Любая информация и данные в электронном, цифровом или физическом форматах (печатная или представленная в ином виде), размещенная, хранящаяся или используемая в или на помещениях, оборудовании, сетях или системах компании PepsiCo. Информация используется как синоним «информационных ресурсов» и «данных».
Владелец информации	См. Раздел 1.2 настоящего документа.
Пароль	Частная или секретная последовательность символов, используемая для аутентификации личности пользователя как средство ограничения доступа к системе только для уполномоченных Сотрудников.
PepsiCo	Собирательное понятие для всех корпоративных дочерних предприятий и филиалов компании PepsiCo Inc. и ее совместных или аффилированных предприятий, включая без ограничения Frito-Lay North America (FLNA), PepsiCo Beverages and Food (PBF) и PepsiCo International (PI).
Частная сеть компании PepsiCo	Включает объекты, принадлежащие и используемые компанией PepsiCo (т.е. проводка, сегменты LAN, маршрутизаторы, выключатели и т.д. на объектах компании PepsiCo), и объекты, полученные от поднадзорных зарегистрированных частных компаний-владельцев сети связи, если логический канал передачи данных доступен только для компании PepsiCo.
Удаленный доступ	Любой доступ к частной сети компании PepsiCo, который не осуществляется посредством прямого проводного физического соединения с сегментом локальной сети, являющимся частью частной сети компании PepsiCo.
Сторонний сотрудник	Лицо, не являющееся сотрудником. «Сторонний» также относится к организации, которая не принадлежит компании PepsiCo.
Идентификатор пользователя	Уникальный символ или последовательность символов, используемый системой для идентификации определенного пользователя (Сотрудника).
Виртуальная частная сеть (VPN)	Частная сеть передачи данных, которая использует «туннель» (или путь) для передачи данных на инфраструктуру связи общего пользования. Для защиты конфиденциальности данные шифруются перед отправкой через сеть общего пользования и расшифровываются при получении. Адреса исходящей и входящей сетей также могут зашифровываться.