«Утверждаю»
_____

«__» «_____» 20__ г.

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА
ЗАЩИТА ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Содержание

1 Назначение и область применения

1.1 Настоящая документированная процедура устанавливает единые требования по обеспечению информационной безопасности всех информационных систем АО «ПРИМЕР» (далее-компания) в части их защиты от вредоносного программного обеспечения.

1.2 Настоящая документированная процедура является внутренним нормативным документом компании.

1.3 Требования настоящей документированной процедуры распространяются на всех работников компании, использующих средства обработки информации.

2 Нормативные ссылки

1.4 В настоящей документированной процедуре приведены ссылки на следующие нормативные документы:

……

3 Термины и определения

1.5 В настоящей документированной процедуре компании применяются термины л соответствующие им определения.

Закон РК	«Об электронном документе и электронной цифровой подписи»;
ISO/IEC 27001:2022	Информационные технологии, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования
ISO/IEC 27002:2022	Информационная безопасность, кибербезопасность и защита конфиденциальности. Управление информационной безопасностью
……..	……
……..	……

4 Сокращения и обозначения

4.1 В настоящей документированной процедуре применены сокращения и обозначения в соответствии с таблицей 1.

Таблица 1. Сокращения и обозначения

№ п/п	Сокращения и обозначения	Полное наименование приведенных сокращений и обозначений
1	АВЗ	Антивирусная защита
3	ИА	Информационный актив
4	ИБ	Информационная безопасность
5	ИС	Информационная система
6	кцд	Конфиденциальность, целостность, доступность
7	ПО	Программное обеспечение
8	САЗ	Система антивирусной защиты

4 Ответственность и полномочия

5.1 Ответственность за разработку настоящей документированной процедуры несет ……

5.2 Ответственность за управление настоящей документированной процедурой несет ……. и ответственное подразделение (лицо).

5 Требования

С целью обеспечения конфиденциальности, целостности и доступности информации и программного обеспечения компанией принимаются меры по защите ИА и ИС от вредоносного программного обеспечения, мобильного кода и нежелательной электронной почтовой корреспонденции (спам) в соответствии с требованиями настоящей документированной процедуры.

5.1 Методы защиты ИА и ИС от вредоносного ПО

5.1.1 Для защиты от вредоносного ПО в компании применяются организационные меры и

технические решения согласно данному разделу настоящей документированной процедуры.

5.1.2 Для снижения рисков проникновения вредоносного ПО в ИС через технические уязвимости ПО, в компании применяется процедура управления техническими уязвимостями в соответствии с требованиями документированной процедуры «Порядок управления техническими уязвимостями информационных систем».

5.1.3 Для защиты средств обработки информации и своевременного блокирования вредоносного ПО в компании применяется Система Антивирусной Защиты.

5.1.4 САЗ должна обеспечивать защиту от проникновения вредоносного ПО в корпоративные ИС компании, как минимум, по следующим каналам:

1) локальные и глобальные коммуникационные сети;
2) съемные носители информации;
3) электронная почта;
4) системы обмена мгновенными сообщениями.

5.1.5 Антивирусное ПО устанавливается на всех средствах обработки информации, где существует техническая возможность установки такого ПО. Исключения из данного требования документально оформляются Менеджером соответствующей ИС, с обоснованием причин исключения средства обработки информации из САЗ.

5.1.6 САЗ должна обеспечивать возможность:

1) централизованного управления, обновления антивирусного ПО, установленного на рабочих станциях пользователей;
2) мониторинга состояния событий антивирусного ПО;
3) оповещения Менеджера АВЗ о событиях ИБ.

5.1.7 Настройки ПО САЗ должны отвечать следующим требованиям:

1) обновление баз вирусных сигнатур производиться не реже одного раза в сутки;
2) доставка обновлений баз вирусных сигнатур и ПО производится незамедлительно после получения данных обновлений системой обновления САЗ;
3) мониторинг возможных каналов проникновения вредоносного ПО на всех средствах обработки информации производиться в режиме реального времени;
4) не реже одного раза в неделю производится полная проверка средств обработки информации на предмет наличия вредоносного ПО;
5) пользователи средств обработки информации не имеют возможность отключения или изменения настроек антивирусного ПО;
6) пользователи имеют возможность инициировать частичную или полную проверку средства обработки информации на предмет наличия вредоносного ПО, в случае наличия у них подозрений о наличии в системе вредоносного ПО;
7) при наличии в антивирусном ПО средств эвристического анализа исполняемого кода, данная функция активирована для защиты от вредоносного ПО, не занесенного в базы вирусных сигнатур.

5.1.8 Для мобильных устройств, не имеющих постоянного подключения к САЗ, применяется настройка, при которой при подключении мобильного устройства во внутреннюю телекоммуникационную сеть, данное устройство автоматически перенаправляется в специальную карантинную зону, изолированную от Продуктивной Среды ИС, до тех пор, пока не будет проверено наличие на этом устройстве антивирусного ПО и актуальности обновлений баз вирусных сигнатур. В случае выявления несоответствий, все необходимые обновления автоматически устанавливаются на мобильное устройство с последующим перенаправлением устройства в Продуктивную Среду ИС.

5.1.9 Ответственность за управление САЗ, мониторинг событий и реагирование на инциденты, связанные с вредоносным ПО, несет Менеджер АВЗ. Порядок управления инцидентами ИБ, связанными с вредоносным ПО, предусматривается документированной процедурой «Порядок управления инцидентами информационной безопасности».

5.1.10 Требования и процедуры по восстановлению ИС в случае нарушения ее работы вредоносным ПО отражаются в Планах восстановления всех ИС в соответствии с требованиями Процедуры об управлении непрерывностью деятельности.

5.1.11 Для контроля и защиты возможных каналов проникновения вредоносного ПО в компании применяются следующие документированные процедуры:

1) управление доступом и использованием локальных и глобальных коммуникационных сетей осуществляется согласно требованиям документированной процедуры «Обеспечение безопасности сетевых сервисов»;
2) управление порядком использования съемных носителей информации осуществляется в соответствии с требованиями Процедуры о носителях информации (ПР-70-05);

3) управление порядком обмена информацией, включая обмен сообщениями электронной почты и мгновенными сообщениями, осуществляется в соответствии с требованиями документированной процедуры «Обеспечение безопасности при обмене информацией» (ДП-50- 17).

5.2 Методы защиты ИА и ИС от мобильного кода

5.2.5 Использование мобильного кода разрешается только для осуществления работниками компании своих должностных обязанностей. В остальных случаях использование мобильного кода ограничивается настройками политики безопасности применяемого ПО.

5.2.6 Анализ рисков информационной безопасности, связанных с применением мобильного кода, проводится в соответствии с документированной процедурой «Порядок оценки и обработки рисков информационной безопасности» с применением контрольных мер для снижения этих рисков до приемлемого уровня.

5.2.7 Для исполнения мобильного кода применяется только ПО, утвержденное ответственным лицом для использования в компании.

Настройки политики безопасности ПО, применяемого для исполнения мобильного кода, должны отвечать следующим требованиям:

1) программным обеспечением исполняется только мобильный код, полученный из доверенных источников. Перечень доверенных источников составляется и поддерживается в актуальном состоянии Менеджером ИС, посредством которого предоставляется доступ к источникам мобильного кода. Мобильный код, полученный не из доверенных источников, блокируется для данного ПО своевременно применяются все обновления безопасности в соответствии с требованиями документированной процедуры «Порядок управления техническими уязвимостями информационных систем»;

2) установка прoграммного обеспечения, полученного посредством мобильного кода выполняется только специалистами службы технической поддержки.

5.2.8 Па рабочих станциях устанавливается и регулярно обновляется антивирусное ПО. Функциональные возможности антивирусного ПО обеспечивают проверку исполняемого мобильного кода в режиме реального времени на предмет наличия в его составе вредоносного ПО.

5.3 Методы защиты от спама

5.3.5 Для снижения нагрузки на телекоммуникационные каналы, повышения эффективности работы персонала компании и снижения рисков разглашения конфиденциальной информации в компании применяются организационные меры и технические решения согласно данному разделу настоящей документированной процедуры.

5.3.6 В компании применяются средства фильтрации нежелательной входящей электронной почтовой корреспонденции (спама). Ответственность за сопровождение и мониторинг данных средств несет Менеджер ИС корпоративной электронной почты.

5.3.7 Политика фильтрации входящих сообщений электронной почты должна отвечать следующим требованиям:

1) обеспечиваться фильтрация сообщений электронной почты отправленных от имени несуществующего электронного почтового ящика;

2) обеспечиваться фильтрация сообщений электронной почты отправленных от имени электронного почтового ящика, занесенного в «черный список» средств фильтрации спама;

3) обеспечиваться фильтрация сообщений электронной почты отправленных серверов электронной почты занесенных в «черный список» средств фильтрации спама;

4) не выполняться фильтрация сообщений электронной почты отправленных от имени электронного почтового ящика и/или почтового домена, занесенного в «белый список» средств фильтрации спама;

5) производиться анализ содержания сообщений электронной почты и обеспечивается их фильтрация на основании правил фильтрации по содержанию (контентной фильтрации).

5.3.8 Ответственность за соблюдение политики фильтрации входящих сообщений электронной почты, а также ведение «черного» и «белого» списков фильтрации и правил контентной фильтрации несет Менеджер ИС корпоративной электронной почты.

5.4 Методы защиты от прочих угроз, связанных с вредоносным ПО

5.4.1 Для предотвращения разглашения конфиденциальной информации в связи с мошенническими действиями третьих лиц с применением средств электронной почты и сервисов обмена мгновенными сообщениями, до сведения всех работников компании, имеющих доступ к данным средствам обмена

информацией, Менеджером ИС корпоративной электронной почты должны быть доведены следующие сведения:

1) работниками компании не предоставляется никакая информация о компании в ответ на запрос третьих лиц, полученный посредством электронных средств обмена информацией, пока не будет достоверно установлено, что данное лицо имеют право на получение данной информации в соответствии с требованиями документированной процедуры «Обеспечение конфиденциальности данных информационных систем»;

2) работники компании не отвечают на подозрительные электронные почтовые сообщения, полученные от неизвестных отправителей, поскольку ответ на такое сообщение подтверждает факт наличия и активного использования адреса электронной почты, что может быть в дальнейшем использовано для проведения несанкционированных рассылок спама и иных атак на ИС компании;

3) при санкционированном компанией использовании работником внешних ИС, требующих предоставления конфиденциальной информации компании, работник удостоверяется в подлинности данной ИС путем сверки электронного адреса ИС с предоставленным ее владельцем.

5.5 Осведомленность работников компании

5.5.1 Для снижения рисков, связанных с вредоносным ПО, мобильным кодом, спамом Менеджер АВЗ регулярно проводит обучение пользователей ИС о порядке и методах защиты от вредоносного ПО.

6 Записи

6.1 В настоящей документированной процедуре формируются следующие записи (таблица 2) которые должны управляться в соответствии с требованиями документированной процедуры «Управление записями».

Таблица 2. Перечень записей

№ п/п	Наименование	Форма записей	Ответственно сть за ведение записей	Хранение место	Периодичность составления записи
1	Регистрация событий антивирусного ПО	Журнал событий в зависимости от ПО. Записи могут	Ответственные за ПО лица		по мере необходимости
		формироваться автоматически посредством соответствующих информационных систем в электронном виде.			
2	Политика подключения мобильных устройств, не имеющих постоянного подключения к САЗ, во внутреннюю телекоммуникационную сеть компании	В зависимости от ПО	Ответственные за ПО лица		по мере необходимости
3	Политика фильтрации входящих сообщений	В зависимости от ПО	Ответственные за ПО лица		по мере необходимости

7 Пересмотр, внесение изменений, хранение и рассылка

7.1 Пересмотр (актуализация), внесение изменений, хранение и рассылка настоящей документированной процедуры осуществляется в соответствии с требованиями документированной процедуры «Управление документацией».

7.2 «Оригинал» в бумажном виде настоящей документированной процедуры хранится в ……

7.3 Учтенные бумажные копии настоящей документированной процедуры при необходимости, рассылаются в заинтересованные структурные подразделения компании.

Лист регистрации изменений

Номер изменения	Номера страниц	Всего листов в документе	Номера разделов, к которым относятся изменения	Описание изменений	Отметка о внесении изменений		
					Ф.И.О.	Подпись	Дата
					-		

Лист ознакомлении

№ п / п	Ф. И. О.	Должность	Дата	Подпись
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				