Приложение 2

Оценка уровня информационной безопасности

(уровень расширенный)

Наименование партнера:

Контактная информация:

Дата заполнения:

Инструкция по заполнению:

Все области с синим форном обязательны для заполнения.
В случае, если какое-либо требование является не актуальным для Вашей организации, то Вы можете проставить значение N\A с обязательным указанием причины в поле "Комментарий".

Итоговый уровень информационной безопасности оценивается для следующих областей:
1. Идентификация, аутентификация, доступы.
2. Регистрация событий.
3. Антивирусная защита.
4. Обновление программного обеспечения.
5. Правила защиты информации для сотрудников.
6. Физическая безопасность.
7. Защита сети.
8. Организация и менеджмент ИБ.
9. Шифрование данных.

Итоговая оценка:

	Процент выполнения	Не выполнены	Выполнены	N\A	Без ответа
Уровень ИБ	0,0%	0	0	0	

Трансграничная передача	Нет

	ИТОГОВАЯ СТАТИСТИКА
0	Количество вопросов **"без ответа"**
0	Количество ответов **"N\A"**
0	**"Выполнено"**
0	**"Не выполнено"**

ИТОГ: 0,0%

№ п/п	Рекомендация	Статус	Уровень важности	Комментарии
1. Идентификация, аутентификация, доступы				
1.1	Каждому пользователю присвоен уникальный логин и пароль для входа в систему?		2	

1.2	Контролируется ли срок действия пароля пользователя в системе?		1	
1.3	Контролируется ли сложность создаваемого пароля пользователя в системе?		2	
1.4	Контролируется ли количество неверных попыток ввода пароля пользователем в систему?		1	
1.5	Контролируется ли количество предыдущих паролей, используемых пользователем в системе?		1	
1.6	Блокируется ли доступ к системе по достижению заданного количества неправильно введенных паролей?		1	
1.7	Доступы сотрудникам организации предоставляются с учетом принципа наименьших привилегий?		1	
1.8	Имеется ли в организации список пользователей с привилегиями высокого уровня (например, root, administrator и т.д.)?		1	
1.9	Ограничиваются ли для сотрудников организации доступы к внешним устройствам и портам?		2	
1.10	Ограничиваются ли для сотрудников организации доступы к ресурсам сети Интернет?		2	
1.11	Применяется ли в организации система DLP для контроля передачи данных на внешние email?		1	
1.12	Применяется ли в организации система DLP для контроля передачи данных на облачные хранилища?		1	
1.13	Применяется ли в организации система DLP для контроля передачи данных на внешние носители информации?		1	
1.14	Применяется ли в организации система DLP для контроля передачи данных вовне с помощью интернет-мессенджеров (Skype, WhatsApp, Telegram, Viber и др.)?		1	
1.15	Осуществляется ли блокировка экранов ПК при простое с обязательной аутентификацией пользователей при активации экрана?		2	
2. Регистрация событий				
2.1	Регистрируются ли действия пользователя в системе?		2	
2.2	Регистрируются ли коды (номера операций) выполненного пользователем действия?		2	
2.3	Регистрируется ли дата и время выполненного действия?		2	
2.4	Регистрируется ли идентификатор пользователя, который выполнил действие?		2	

2.5	Регистрируется ли IP-адрес, MAC-адрес устройства доступа (в зависимости от технической возможности)		2	
2.6	Хранятся ли регистрационные данные в течении 5 лет?		1	
2.7	На всех устройствах организации выполняется синхронизация времени с основным источником времени?		2	
2.8	Используется ли в организации централизованное хранилище регистрируемых событий?		2	
2.9	Используется ли в организации специализированная система обработки регистрируемых событий (SIEM)?		2	
3. Антивирусная защита				
3.1	Установлена ли антивирусная защита на всех объектах информационной инфраструктуры?		2	
3.2	Функционирует ли антивирусная система защиты в резидентном режиме?		2	
3.3	Проводится ли полная проверка рабочих станций не реже одного раза в неделю?		2	
3.4	Осуществляется ли обновление антивирусных баз не реже одного раз в день?		2	
3.5	Определена ли в организации процедура реагирования в случае вирусной активности - определены действия пользователей и сотрудников ИБ и ИТ?		2	
3.6	Проверяются ли все вложения электронной почты на наличие вредоносного кода?		2	
3.7	Проверяются ли все внешние носители информации при подключении к ПК на наличие вредоносного кода?		2	
4. Обновление программного обеспечения				
4.1	Осуществляется ли контроль установки критичных обновлений?		2	
4.2	Устанавливаются ли критические обновления, связанные с безопасностью операционных систем и прикладного программного обеспечения.		2	
4.3	Выполняется ли регулярное сканирование инфраструктуры организации для поиска уязвимостей операционных систем и прикладного программного обеспечения для дальнейшей установки критичных обновлений?		2	
4.4	Устанавливаются ли общие обновления прикладного и системного программного обеспечения.		1	

4.5	Осуществляется ли в организации обновление ПО, в том числе критические обновления ИБ, сетевых экранов, систем IDS, IPS и др.?		2	
5. Правила защиты информации для сотрудников				
5.1	Разработан ли документ, регламентирующий правила защиты информации для сотрудников?		2	
5.2	Определены ли в документе правила использования паролей?		2	
5.3	Определены ли в документе правила работы в сети Интернет?		1	
5.4	Определены ли в документе правила работы с конфиденциальной информацией (персональные данные, коммерческая тайна)		2	
5.5	Определены ли в документе правила работы с внешними накопителями информации		1	
5.6	Определены ли в документе правила обработки конфиденциальной информации на бумажных носителях информации?		2	
5.7	Определены ли в документе правила работы с персональными компьютерами?		1	
5.8	Определена ли в организации информация, которая является конфиденциальной для организации?		1	
5.9	Определена ли в документе ответственность сотрудников за не исполнение правил защиты информации?		2	
5.10	Ознакомлены ли сотрудники с правилами защиты информации?		2	
6. Физическая безопасность				
6.1	Организован ли в организации пропускной режим (ограничение доступа в помещения организации)?		1	
6.2	Ограничен ли в организации доступ в серверные помещения и другие помещения, в которых размещается серверное, коммутационное и др. оборудование?		2	
6.3	Имеется ли в организации система охранной сигнализации/система сигнализации вторжения с круглосуточным контролем?		1	
6.4	Имеется ли в организации система видеонаблюдения?		1	
6.5	Хранятся ли записи с системы видеонаблюдения не менее 90 дней?		1	
6.6	Выполняется ли уничтожение данных с носителей, информация на которых должна уничтожаться?		1	
7. Защита сети				

7.1	Используются ли в организации для защиты сетевой инфраструктуры сетевые экраны?		2	
7.2	Используются ли в организации для защиты сетевой инфраструктуры системы IPS, IDS и др.?		2	
7.3	Имеется ли в организации актуальная документация по конфигурации сети с указанием схемы и описанием?		2	
7.4	На сетевых устройствах (маршрутизаторы, сетевые экраны, IDS, IPS и т.д.) отключены небезопасные протоколы (telnet, SNMP v1)?		2	
7.5	Изменены ли в организации на сетевых устройствах и в системах пароли по умолчанию на новые стойкие пароли?		2	
7.6	Настроены ли сетевые экраны в организации по принципу - запрещено все, что не разрешено?		2	
7.7	Осуществляется ли в организации блокировка вредоносных сайтов и загрузка вредоносных файлов?		1	
7.8	Для удаленного доступа к информационным ресурсам организации всегда используется двухфакторная аутентификация?		1	
7.9	Если в организации используется беспроводная сеть ЛВС, то точки доступа Wi-Fi располагаются в выделенной зоне DMZ?		1	
7.10	Если в организации используется беспроводная сеть ЛВС, то на всех точках доступа настроено шифрование WPA/WPA2?		1	
7.11	Если в организации используется беспроводная сеть ЛВС, то для доступа к информационным ресурсам организации из подсети Wi-Fi необходима аутентификация пользователя?		2	
7.12	Проводится ли тестирование работы резервного канала связи как минимум один раз в квартал?		2	
7.13	Настроена ли в организации сегментация сети с настройкой доступов между сегментами сети с помощью сетевых экранов?		1	
7.14	Проводятся ли в организации тесты на проникновение?		1	
8. Организация и менеджмент ИБ				
8.1	Имеется ли в организации отдельное подразделение информационной безопасности или сотрудники, отвечающие за информационную безопасность, обладающие необходимой квалификацией?		2	
8.2	Определены ли в организации регламентные документы по ИБ (Политика информационной безопасности, положения, стандарты, инструкции в области ИБ)?		2	

8.3	Актуализация регламентных документов в области ИБ осуществляется не реже, чем один раз в 2 года?		1	
8.4	Все ли сотрудники перед устройством на работу проходят обучение/инструктажи по вопросам ИБ?		2	
8.5	Проводятся ли в организации учения/проверки по выполнению требований ИБ (например, рассылка тестовых фишинговых писем)?		1	
8.6	Определена ли в организации процедура управления рисками ИБ?		1	
8.7	Проводился ли в организации в течение последних 2 лет аудит в области ИБ (собственными силами или сторонней организацией)?		1	
8.8	Определена ли в организации процедура реагирования на инциденты ИБ и ИТ?		1	
8.9	Имеется ли в организации отдельное подразделение (или уполномоченные сотрудники) оперативного реагирования на инциденты ИБ (SOC)?		1	
8.10	Возможно ли, что конфиденциальные данные, передаваемые из организации, будут пересекать гос. границу РФ, т.е. будет осуществляться трансграничная передача данных (возможно из-за соображений маршрутизации)?		2	
9. Шифрование данных				
9.1	Осуществляется ли в организации шифрование данных при передаче конфиденциальной информации по открытым каналам связи (использование шифрованных каналов связи https, sftp и т.д. или шифрование самих данных)?		2	
9.2	При отправке писем, содержащих конфиденциальную информацию, используется ли шифрование?		1	
9.3	Осуществляется ли шифрование данных на ноутбуках сотрудников организации (например, Bitlocker)?		1	
9.4	Определен ли в организации порядок использования, хранения, учета ключей шифрования?		1	