**Запрос информации по Проекту**

**«Проведение комплексного аудита**

**информационной безопасности Группы компаний АФК «Система»»**

**Обзор проекта:**

ПАО АФК «Система» рассматривает возможность реализации проекта **«Проведение комплексного аудита информационной безопасности Группы компаний АФК «Система»» (далее – «Аудит»).**

Требования к составу и содержанию работ указаны в Требованиях (Приложение 2) к настоящему документу.

**Планируемый график реализации Проекта:**

Группа компаний АФК «Система» планирует начать работы во второй половине 2021 года, а завершить их не позднее 1 полугодия 2022 года.

**Предложение и процесс запроса информации:**

Мы ожидаем получить краткое предложение, которое должно включать:

* порядок проведения и описание работ по проведению Аудита в разрезе выполнения основных требований – в формате презентации/пояснительной записки (на выбор);
* предполагаемый объем необходимых работ с оценкой трудозатрат по каждому из этапов (в чел./час.) за единицу обследования по двум возможным Типам – в формате Приложения 1, лист «Основные этапы и Ценовое предложение»;
* предложение по цене (в рублях) с учетом применимого НДС, с указанием стоимости по каждому из этапов за единицу проведения (внешний узел, сервер, рабочая станция, отчетная документация и т.п.) по каждому Типу – в формате Приложения 1, лист «Основные этапы и Ценовое предложение»;
* краткий обзор аналогичных/сопоставимых реализованных проектов;
* данные о ключевых членах предполагаемой проектной команды с указанием их профессионального опыта и функциональных ролей в Аудите – в формате Приложения 1, лист «Команда проекта».

**ВНИМАНИЕ!!!** Подача документов осуществляется Участником в электронном виде через электронно-торговую площадку (далее - «ЭТП») по адресу http://utp.sberbank-ast.ru/VIP/List/PurchaseList/358 в соответствии с регламентом и инструкцией для Участников торговой секции «Закупки и продажи» универсальной торговой платформы «Сбербанк-АСТ», ознакомиться с которыми можно на сайте <http://utp.sberbank-ast.ru/VIP/Notice/752/Information>.

Срок окончания подачи документов на участие и коммерческих предложений «17» июня 2021г. до 19.00 часов (МСК). **Документы и предложения, поданные после указанного срока, ЭТП не принимаются.**

**Общий объем Аудита:**

Количество компаний (площадок), планируемых к обследованию – 29

Оценочное количество обследуемой инфраструктуры:

* Внешние узлы – более 1700
* Рабочие станции – более 36 тыс.
* Сервера – более 4 тыс.

Вы можете направить интересующие Вас вопросы через ЭТП и/или следующим контактным лицам:

|  |  |
| --- | --- |
| **Зайцев Алексей**  ПАО АФК «Система»  Директор по эксплуатации систем информационной безопасности  Тел.: +7 495 692 10 88, доб. 50390  e-mail: a.zaytsev@sistema.ru |  |

**Важная информация (Disclaimer)**

ПАО АФК «Система» уведомляет, что настоящий запрос информации не должен расцениваться потенциальными исполнителями в качестве публичной оферты ПАО АФК «Система». ПАО АФК «Система» не несет никаких обязательств перед компаниями, принявшими участия в данном запросе информации, и может прекратить проект в любой момент времени.

**Приложения:**

Приложение 1. Анкета участника и форма ценового предложения



Приложение 2. Требования к проведению комплексного аудита информационной безопасности Группы компаний АФК «Система».

**Приложение 2**

**Технические требования**

**к проведению комплексного аудита информационной безопасности**

**Группы компаний АФК «Система»**

1. **Общие положения**
   1. Наименование работ

Полное наименование: комплексный аудит информационной безопасности.

Сокращение в тексте: Аудит ИБ.

* 1. Список условных обозначений и терминов

ГОСТ – государственный стандарт

ИБ – информационная безопасность

ИС – информационная система

ПО – программное обеспечение

1. **Цель и задачи оказываемых услуг**

Целью оказания услуг является получение объективной и независимой оценки текущего уровня информационной безопасности (далее – ИБ) информационных систем (далее – ИС) Заказчика, выявление и практическая верификация недопустимых киберсобытий, оценка киберрисков и их последствий, определение приоритетных направлений развития информационной безопасности.

Достижение указанных целей обеспечивается решением следующих задач:

определение недопустимых для Заказчика киберсобытий и практические семинары для руководства Заказчика;

верификация реализуемости недопустимых событий в реальных условиях Заказчика и проверка фактического потенциала Заказчика по противодействию кибератакам;

сбор и анализ исходных данных об информационных системах, используемых средствах защиты информации и процессах ИБ;

интервьюирование владельцев бизнес-процессов для установления актуальных рисков и определения критичности последствий их реализации;

оценка текущего уровня зрелости процессов обеспечения ИБ;

определение результатов развития информационной безопасности и формирование целевого состояния;

разработка рекомендаций по повышению уровня ИБ ИС и Стратегии развития информационной безопасности, содержащей карточки проектов и дорожную карту инициатив, а также эскизные проекты и технические требования;

подготовка материалов для коллегиального утверждения Стратегии развития ИБ и ее финансирования.

1. **Состав и содержание работ**

Работы должны проводиться в один этап в следующем порядке:

определение недопустимых киберсобытий и анализ сценариев их реализации;

практическая верификации реализуемости недопустимых киберсобытий и проверка возможностей по противодействию кибератакам;

обследование ИС, включая интервьюирование владельцев ключевых бизнес‑процессов и сбора свидетельств в части обеспечения защиты информации и оценки рисков;

оценка соответствия текущего уровня зрелости процессов обеспечения ИБ применимым требованиям регуляторов и международным стандартам по информационной безопасности и количественная оценка рисков ключевых бизнес-процессов;

технический анализ защищенности активов ИТ инфраструктуры;

построение карты основных рисков и угроз, их ранжирование по величине потенциального ущерба;

актуализация корпоративного стандарта по информационной безопасности ПАО АФК «Система»;

разработка рекомендаций по повышению уровня ИБ и Стратегии развития ИБ;

разработка эскизных проектов и технических требований для Стратегии развития ИБ;

определение способов и ресурсов, необходимых для реализации Стратегии развития ИБ, и подготовка материалов для коллегиального утверждения ее финансирования;

перепроверка устранения выявленных в ходе аудита уязвимостей;

анализ исправления недостатков предыдущих аудитов и тестов на проникновение по направлению информационной безопасности.

* 1. Общие требования к выполнению работ

Перед началом выполнения работ Заказчик формирует Управляющий комитет и Рабочую группу по данному проекту, в состав которых должны быть также включены согласованные представители Исполнителя.

В процессе выполнения работ Исполнитель формирует запросы на предоставление информации, а Заказчик содействует ее сбору и обеспечивает ее предоставление Исполнителю в объеме необходимом и достаточном для качественного выполнения работ.

Рассмотрение и согласование работ и результатов по оказанию услуг осуществляется Рабочей группой проекта. Приемка результатов оказания услуг осуществляется Управляющим комитетом проекта.

Для управления ходом выполнения работ назначаются регулярные встречи Рабочей группы и периодические заседания Управляющего комитета, а также определяется типовой формат отчетности для данных совещаний.

* 1. Требования к содержанию работ по определению недопустимых киберсобытий и анализу сценариев их реализации

Для выполнения данных работ Исполнитель проводит первичное изучение деятельности Заказчика, его структуры, основных показателей, формирует список участников, повестку и дополнительные материалы для интервью с руководителями Заказчика, а также разрабатывает презентационные материалы для вводного семинара.

Перед проведением интервью Исполнитель проводит вводный семинар с руководителями Заказчика и начальниками структурных подразделений Заказчика и предоставляет разъяснения о недопустимых событиях и предстоящих интервью, а также формирует график встреч.

Сведения, предоставленные руководителями Заказчика в ходе интервью с ними, являются основной информацией для формирования перечня недопустимых событий и ущерба. Дополнительно в качестве базы знаний могут применяться имеющиеся у Заказчика значения допустимого ущерба, аппетита к рискам, а также реестры рисков и инцидентов. Для каждого выявленного события должны быть определены характеризующие его количественные параметры.

Выявленные Исполнителем недопустимые киберсобытия должны быть структурированы в виде табличной матрицы с учетом значимости и области ущерба.

Моделирование сценариев реализации недопустимых киберсобытий осуществляется путем формирования логической цепочки действий злоумышленника в сфере цифровых технологий (в киберпространстве) и их последствий. Сценарии реализации недопустимых событий оформляются в виде карточек, содержащих:

наименование и текстовое описание сценария;

ресурсы Заказчика, которые пострадают в результате реализации сценария;

последствия и ущерб в результате реализации сценария.

Разработанные сценарии включаются в программу практического семинара для их рассмотрения и уточнения.

По результатам работ по определению недопустимых событий и анализа сценариев их реализации Исполнитель должен разработать программу и презентационные материалы для практического семинара по разбору сценариев реализации недопустимых событий и обеспечить его проведение. Содержание семинара должно включать:

отраслевую специфику Заказчика и элементы повышения осведомленности в области кибербезопасности;

рассмотрение сценариев реализации недопустимых событий с элементами бизнес-игры;

уточнение недопустимых событий и ущерба;

сбор мнений участников относительно направлений развития ИБ.

Основными участниками семинара будут выступать руководители Заказчика и лидеры по направлениям деятельности Заказчика. Число участников семинара составит не более 20 человек, а его длительность – не более 4х часов.

По результатам практического семинара Исполнитель формирует краткий отчет, а уточненные сценарии реализации недопустимых событий используются в ходе работ по оценке рисков.

* 1. Требования по практической верификации реализуемости недопустимых киберсобытий и проверке возможностей по противодействию кибератакам

Перед началом практической верификации реализуемости недопустимых киберсобытий Исполнитель разрабатывает правила, которые должны содержать:

недопустимые события, подлежащее верификации;

сценарий реализации недопустимого событий;

целевые информационные системы;

критерии успешной верификации;

методы и способы верификации;

методы детектирования действий по верификации недопустимых событий, которые будут применятся Заказчиком;

порядок взаимодействия Исполнителя и Заказчика в ходе верификации;

порядок фиксации действия Заказчика и Исполнителя в ходе верификации.

Для выполнения работ по практической верификации реализуемости недопустимых событий Исполнитель должен сформировать группу, в которую включить специалистов с квалификацией, достаточной для имитации действий злоумышленников различного уровня подготовки, в том числе уровня хакерских группировок с возможностью поиска и эксплуатации ранее неизвестных уязвимостей (уязвимости 0-дня).

Имитация действий кибер-злоумышленников должна быть направлена на достижение критериев успешной верификации, включать мероприятия, перечисленные в данном разделе, и, при необходимости, детализироваться в правилах практической верификации реализуемости недопустимых киберсобытий. Верификация недопустимых событий должна осуществляться с использованием навыков наступательной безопасности (offensive security), этичного хакинга, анализа защищенности, тестирования на проникновение и red-teaming. В ходе данных работ Заказчик использует доступный ему арсенал средств информационной безопасности и фиксирует все обнаружения действий Исполнителя в соответствии с правилами верификации. Перед началом работ Заказчику будет предоставлен список внешних IP-адресов Исполнителя. Предоставление списка внешних IP-адресов Исполнителя необходимо для того, чтобы подразделение, отвечающее за информационную безопасность со стороны Заказчика, смогло своевременно выявить и отличить действия со стороны Исполнителя от возможных действий со стороны реальных злоумышленников. При этом Заказчик не должен блокировать указанные IP-адреса и вносить их в черные списки на средствах межсетевой защиты, поскольку это может привести к невозможности выполнения работ. В случае, если потребуется, чтобы действия Исполнителя в точности соответствовали действиям реальных кибер-злоумышленников, то Заказчик может заранее отказаться от предоставления ему списка внешних IP-адресов Исполнителя. В таком случае Заказчик может осуществлять блокировку любых подозрительных активностей, а Исполнитель может использовать любые IP-адреса для проведения верификации без предварительного согласования с Заказчиком. Данный аспект должен быть согласован до начала проведения работ и включен в правила практической верификации реализуемости недопустимых киберсобытий.

При верификации недопустимых киберсобытий Исполнитель должен руководствоваться применимыми российскими и международными стандартами и подходами, а также использовать собственные методические и программные разработки.

В результате проведения работ должен быть разработан технический отчет о результатах верификации недопустимых киберсобытий.

* 1. Требования к составу и содержанию работ по обследованию ИС

В рамках обследования должны быть собраны сведения о ключевых бизнес-процессах и автоматизирующих их ИС, а также сведения о применяемых организационных и технических мерах защиты, включая:

категории и объем циркулирующей в ИС информации и технологии ее обработки;

перечень ИС, участвующих в бизнес-процессах компании, или взаимодействующих с такими ИС, и уровни их критичности;

состав компонентов ИТ инфраструктуры, обеспечивающих функционирование ИС,

схема сетевой инфраструктуры и сетевые правила доступа;

перечень ролей пользователей и администраторов ИС;

применяемые меры и средства защиты информации в ИС;

планы обеспечения непрерывности бизнеса (BCP) и планы восстановления после аварии (DRP)

действующие организационно-распорядительные документы по обеспечению ИБ;

организационная структура и функциональные обязанности работников Заказчика в части обеспечения ИБ.

Исполнитель должен согласовать с Заказчиком план-график проведения работ, включая определение:

зоны ответственности и порядок коммуникаций между Заказчиком и Исполнителем;

перечень ИС и их компонентов, подлежащих аудиту;

перечень помещений, подлежащих аудиту;

перечень сотрудников, с которыми необходимо провести интервью в рамках аудита.

При сборе данных должны применяться следующие методы получения информации:

анализ предоставленной документарной информации по системе защиты информации;

интервью со специалистами Заказчика по предварительно согласованному графику;

анализ параметров конфигураций и настроек ключевых программных и программно-аппаратных компонентов ИС и средств защиты информации, результатов тестов на проникновение.

В ходе проведения работ должны быть собраны свидетельства проведения аудита ИБ.

Результатом работ является структурированная информация об информационных системах Заказчика, которая документируется в соответствующем разделе Отчета об аудите ИБ.

* 1. Требования к составу и содержанию работ по оценке текущего уровня зрелости процессов обеспечения ИБ

В рамках оценки текущего уровня зрелости процессов обеспечения ИБ должны быть выполнены следующие работы:

разработана и согласована с ПАО АФК «Система» методика оценки текущего уровня зрелости процессов обеспечения ИБ (результаты оценки должно быть в том числе визуализированы в виде диаграмм/графиков) и оценки рисков;

проведение оценки текущего уровня зрелости процессов обеспечения ИБ и оценки рисков.

Разрабатываемая методика должна основываться на лучших российских и международных практиках в области ИБ и учитывать требования регуляторов в области обеспечения информационной безопасности:

Федеральный закон от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 27 июля 2006 года №152-ФЗ «О персональных данных»;

Федеральный закон от 29 июля 2004 года №98-ФЗ «О коммерческой тайне»;

Федеральный закон от 26 июля 2006 года №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

Приказ ФСТЭК России от 18 февраля №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

Приказ ФСТЭК России от 25 декабря 2017 г. №239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.

ISO/IEC 27001:2013 или ГОСТ Р ИСО/МЭК 27001-2006. «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;

ISO/IEC 27005:2018 или ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.»;

ISO 31000:2018 или ГОСТ Р ИСО 31000-2019 «Менеджмент риска. Принципы и руководство.»;

ISO/IEC 31010:2019 или ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска.»;

ETSI TS 102 165-1 V5.2.3 (2017-10) «CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)»;

NIST, SANS, CIS, COBIT, CSF.

Состав нормативной базы, которая будет являться основой для проведения оценки текущего уровня зрелости процессов обеспечения ИБ, должна быть определена Исполнителем и согласована с Заказчиком.

На основании полученных в результате работы данных должны быть выполнены:

оценка выполнения требований законодательства РФ;

оценка эффективности существующих процессов ИБ;

оценка выбора мер защиты информации;

оценка полноты реализации мер защиты информации;

оценка рисков ИБ и уровень допустимого риска (риск-аппетит).

Методика должна учитывать особенности организации Заказчика и позволять демонстрировать динамику изменений текущего уровня зрелости процессов обеспечения ИБ и рисков ИБ при проведении повторных оценок.

В область работ по количественной оценке рисков ИБ ограничена 10 (десятью) ключевыми бизнес-процессами. Перечень процессов, подлежащих анализу, определяется Заказчиком. Оценка рисков осуществляется с использованием матрицы и сценариев недопустимых киберсобытий и с учетом результатов практической верификации реализуемости недопустимых событий.

Результатом работ является оценка текущего уровня зрелости процессов обеспечения ИБ и оценка рисков ИБ, которая документируется в соответствующем разделе Отчета об аудите ИБ.

* 1. Требования к составу и содержанию работ по техническому анализу защищенности активов ИТ инфраструктуры

Работы по выполнению настоящих Технических требований должны предусматривать следующие этапы:

анализ защищенности внешнего периметра;

анализ защищенности внутренней инфраструктуры;

анализ защищенности беспроводных сетей;

оценка осведомленности сотрудников в вопросах информационной безопасности;

оценка устойчивости информационных активов к распределенным атакам типа «отказ в обслуживании»;

оценка реагирования на инциденты информационной безопасности;

подготовка рекомендаций по устранению выявленных уязвимостей;

оценка уровня остаточного риска для ключевых систем и процессов;

оценка уровня зрелости процессов реагирования на инциденты ИБ.

* + 1. Требования к составу работ в рамках анализа защищенности внешнего периметра

уточнение объема работ и перечня входящих в область проекта информационных активов на основе анализа информации из открытых источников;

выявление уязвимостей, присутствующих на ресурсах и сервисах, доступных из сети Интернет, разработка и практическое подтверждение возможности их эксплуатации (внешний нарушитель);

ручной и автоматический анализ ИС с целью выявления возможных точек входа как в данные системы, так и во внутреннюю корпоративную инфраструктуру, и их компрометации (внутренний нарушитель);

в случае успешной компрометации внешнего периметра, по согласованию с Заказчиком, возможно развитие атаки на ресурсы внутренней инфраструктуры;

сбор и обобщение статистических данных по результатам анализа защищенности внешнего периметра.

* + 1. Требования к составу работ в рамках оценки осведомленности сотрудников

подготовка и согласование сценариев атаки;

подготовка и рассылка фишинговых сообщений;

сбор статистических данных по результатам проведенной кампании.

* + 1. Требования к составу работ в рамках анализа защищенности беспроводных сетей

проведение атак на беспроводные сети, в том числе защищенные по стандарту WPA2-Enterprise, с целью определения потенциальных точек входа во внутреннюю инфраструктуру;

создание подложных беспроводных сетей с целью перехвата сессий легитимных пользователей;

сбор статистических данных по результатам анализа защищенности беспроводных сетей.

* + 1. Требования к составу работ в рамках анализа защищенности внутренней инфраструктуры

анализ инфраструктуры в режиме «черного ящика» – от лица потенциального нарушителя, не имеющего легитимного доступа к сети (подрядчики, обслуживающий персонал);

анализ возможности подключения стороннего устройства к корпоративной сети с использованием легко доступных интерфейсов подключения (коридоры, переговорные комнаты и т.п.), изучение и получение доступа к внутренним ресурсам;

анализ инфраструктуры в режиме «серого ящика» – с точки зрения злоумышленника, имеющего базовый доступ к корпоративной сети (работник организации без повышенных привилегий);

попытки получения несанкционированного доступа к конфиденциальной информации и чувствительным компонентам ИТ инфраструктуры, закрепления на внутренних узлах сети.

В рамках данного этапа могут использоваться сведения, полученные в ходе предыдущих этапов.

* + 1. Требования к составу работ в рамках оценки устойчивости информационных активов к распределенным атакам типа «отказ в обслуживании»

атаки, направленные на исчерпание полосы пропускания сетевых каналов;

атаки, направленные на исчерпание ресурсов компонентов ИС;

атаки, направленные на механизмы обработки запросов и данных.

Тесты должны проводятся сериями, с постепенно нарастающей нагрузкой (10%, 25%, 50%, 75%, 100%) от согласованного с Заказчиком предельного уровня нагрузки.

* + 1. Требования к составу отчетной документации по этапу технического анализа защищенности

Полученные в результате технического анализа защищенности данные должны быть представлены в соответствующем разделе Отчета об аудите ИБ и содержать следующую информацию:

общие сведения и описание процесса проведения анализа;

описание методики проведения анализа защищённости;

результаты проведённых проверок;

выводы (как развёрнутые технические, так и более краткие для руководства);

оценку состояния защищённости информационных активов Заказчика как с точки зрения потенциальных векторов проникновения, так и с точки зрения используемых механизмов защиты;

перечень и описание выявленных нарушений защиты информации;

перечень представителей со стороны Заказчика, которые сопровождали исполнителя;

описание хода работ, выявленных уязвимостей, степени потенциальной опасности, вероятности их использования, описание последствий реализации выявленных уязвимостей. Все наблюдения должны быть рассмотрены с точки зрения влияния на бизнес-процессы Заказчика и ранжированы в соответствии с актуальными рисками, выявленными в ходе выполнения работ по этапам 3.1-3.3.

формирование конкретных практических рекомендаций по устранению выявленных уязвимостей, в том числе рекомендации по изменению конфигурации и настроек оборудования, используемых защитных механизмов и программных средств, принятию дополнительных мер и применению дополнительных средств защиты, по установке необходимых обновлений для используемого программного обеспечения;

рекомендации по доработке локальных актов Заказчика;

формирование общих методических рекомендаций по модификации существующих процессов администрирования, разработки и/или аутсорсинга разработки систем Заказчика, их администрирования, направленных на минимизацию количества аналогичных недостатков в дальнейшем;

подготовка рекомендаций по совершенствованию защиты информации;

формирование отчета о найденных уязвимостях, способах их эксплуатации и рекомендации по их устранению, результаты эксплуатации нескольких критически опасных уязвимостей, включая информацию о полученном уровне привилегий в активах на различных этапах тестирования.

* + 1. Ограничения

запрещается использовать методы социальной инженерии на всех этапах, кроме социологического исследования без согласования с Заказчиком;

запрещается проводить атаки на учетные записи легитимных клиентов Заказчика, без согласования с Заказчиком;

без предварительного согласования запрещается проводить атаки на учетные записи администраторов и прочих сотрудников поддержки Заказчика;

тесты, которые могу нарушить доступность систем Заказчика или логику ее функционирования, должны быть согласованы отдельно в устанавливаемом Заказчиком порядке.

* 1. Требования к составу и содержанию работ актуализация корпоративного стандарта по информационной безопасности ПАО АФК «Система»

Актуализация корпоративного стандарта по информационной безопасности ПАО АФК «Система» должна вестись с учетом действующих требований законодательства в области обеспечения информационной безопасности, а также с учетом требований регуляторов в области информационной безопасности, включая ФСТЭК России, ФСБ России, Центральный Банк Российской Федерации, международных стандартов и пр.

Актуализированный стандарт по информационной безопасности должен включать в себя в том числе:

определение области применения;

фиксацию базовых требований к обеспечению информационной безопасности;

модель процессов и архитектуры информационной безопасности;

описание требований к обеспечению информационной безопасности по каждому направлению защиты.

* 1. Требования к составу и содержанию работ по разработке рекомендаций по повышению уровня ИБ и разработке Стратегии развития ИБ

В ходе проведения работ по разработке рекомендаций по повышению уровня ИБ должны быть выполнены работы по анализу результатов определения и верификации недопустимых киберсобытий, обследования ИС, оценки текущего уровня ИБ и анализа киберрисков.

При определении рекомендаций должны быть рассмотрены ключевые процессы ИБ, включая следующие процессы:

управление рисками ИБ;

внутренний аудит ИБ;

организация защиты информации;

управление доступом к информации;

физическая безопасность;

защита от вредоносного ПО;

резервное копирование;

контроль за используемым ПО;

управление уязвимостями;

управление внесением изменений в состав ИС;

мониторинг событий ИБ;

управления инцидентами ИБ;

сетевая безопасность;

управление эффективностью и отчетностью ИБ;

управление конфигурациями;

управление навыками безопасного поведения.

Рекомендации по повышению уровня ИБ ИС должны включать:

состав организационных и технических мероприятий по повышению уровня ИБ;

рекомендации по приоритетам реализации проектов по ИБ;

бюджетную оценку проектов по ИБ.

По результатам работ должны быть разработаны рекомендации по повышению уровня ИБ, которые документируются в соответствующем разделе Отчета об аудите, а также подготовлена Стратегия развития ИБ.

Стратегия развития ИБ должна регламентировать:

цели и задачи развития ИБ;

принципы и результаты развития ИБ;

организационно-функциональную модель ИБ;

ключевые направления развития ИБ (проекты ИБ);

по каждому проекту должны быть определены: состав мероприятий, ожидаемый бизнес-результат от реализации проекта, сроки реализации проекта и бюджетная оценка работ;

оценку рисков ИБ в результате реализации Стратегии развития ИБ;

оценку ресурсов, необходимых для реализации Стратегии развития ИБ;

эскизные проекты и требования к техническим мероприятиям;

приоритезированный план-график (дорожная карта) реализации Стратегии развития ИБ.

Стратегия развития ИБ должна быть оформлена в виде и формате, пригодном для рассмотрения и утверждения Заказчиком, а также содержать сведения, необходимые для выделения финансирования на ее реализацию.

* 1. Требования к составу работ в рамках перепроверки устранения выявленных уязвимостей

По истечении 3 месяцев с даты согласования Отчета об Аудите Исполнитель должен провести повторное обследование инфраструктуры Заказчика на предмет оценки успешности устранения выявленных уязвимостей. Проверке подлежат все недостатки, зафиксированные в Отчете. Работы должны проводиться в ручном и автоматизированном режиме с применением методов, используемых Исполнителем в ходе проведение первичного обследования. По письменной договоренности Заказчика и Исполнителя указанные работы могут быть проведены в другие согласованные сроки.

1. **Требования к документированию**

Разработанные отчетные материалы представляются Заказчику в электронном виде (формат: \*.pdf; \*.docx, \*.vsd и других) и на бумажном носителе в сброшюрованном виде, в одном экземпляре.

Отчетные документы должны быть заверены штампом организации Исполнителя и подписями руководителей и работников, ответственных за выполнение услуг.

Разработанные документы должны предоставляться на русском языке.

1. **Требования к Исполнителю**

5.1. Исполнитель должен обладать действующей лицензией ФСТЭК России на деятельность по технической защите конфиденциальной информации.

5.2. Наличие у Исполнителя подтвержденного опыта по успешному проведению аудитов информационной безопасности и/или обследований информационных систем (не менее 3 проектов за последние 3 года).

5.3. Наличие в штате не менее трех специалистов, имеющих подтвержденную квалификацию (диплом о высшем образовании государственного образца) в области обеспечения информационной безопасности и обладающих опытом выполнения соответствующих проектов или иное высшее образование и стаж работы в области оказываемых услуг не менее 5 лет и прошедшего обучение по программам профессиональной переподготовки по одной из специальностей в области информационной безопасности (нормативный срок обучения – не менее 360 аудиторных часов).

Наличие в штате не менее одного специалиста со свидетельством и (или) сертификатом аудитора/ведущего аудитора ISMS (Information Security Management System) по стандарту ISO 27001.

Наличие в штате не менее 3 специалистов, обладающих валидной сертификацией CEH, OSCP, OSWP или аналогами.

Срок деятельности Исполнителя в области оказания услуг по информационной безопасности должен быть не менее 5 лет.

1. **Конфиденциальность**

При взаимодействии между Сторонами подписывается соглашение о неразглашении конфиденциальной информации.

Стороны в полной мере осознают критичность информации, как исходных данных, так и результатов услуг. В ходе оказания услуг специалисты Исполнителя не должны предпринимать каких-либо действий, которые могут привести к уничтожению или блокированию информационных активов Заказчика.