Аналитическая записка

О соответствии текущих функциональных возможностей ПК «АльфаДок» требованиям Указа Президента Российской Федерации № 250 от 01.05.2022 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» и их дальнейшем развитии в целях полноценного исполнения требований данного Указа.

1 мая 2022 года в силу вступил Указ Президента Российской Федерации № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Каким образом ПК «АльфаДок» помогает пользователям выполнить требования этого указа уже сейчас и что планируется в дальнейшей разработке сервиса? Давайте разберем по пунктам.

Пункт 1, пп. а): возложить на заместителя руководителя органа (организации) полномочия по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

Аналогичный по своей сути документ в рамках ПК «АльфаДок» уже разрабатывается - Приказ об ответственном за обеспечение безопасности КИИ (пункт выполняется на тарифах КИИ за счет определения ответственного за обеспечение безопасности КИИ - шаг "Ответственные за обеспечение безопасности КИИ" вкладки "Ответственные" раздела "Ввод данных (ИБ)").

С целью обеспечения согласованности с Указом в преамбулу и тексте приказа в ближайшее время будут внесены корректировки:

1. Появится ссылка на Указ, скорректируется наименование ответственного;

2. По факту утверждения Правительством типового положения о заместителе руководителя органа (организации), ответственного за обеспечение информационной безопасности, в состав приказа приложением будет включено положение об ответственном;

3. Изменяться условия доступности к назначению данного лица для различных тарифов/лицензий (не только на тарифах КИИ).

Пункт 1, пп. б): создать в органе (организации) структурное подразделение, осуществляющее функции по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и

реагированию на компьютерные инциденты, либо возложить данные функции на существующее структурное подразделение.

Аналогичный по своей сути документ в рамках ПК «АльфаДок» уже разрабатывается - Приказ об ответственном за обеспечение безопасности ПДн / за защиту информации (пункт выполняется на тарифах ПДн и ГИС за счет определения ответственного, функции которого возложены на структурное подразделение - шаг «Ответственный за обеспечение безопасности ПДн / защиту информации» вкладки «Ответственные» раздела "Ввод данных (ИБ)").

С целью обеспечения согласованности с Указом в ближайшее время будут внесены корректировки в приказы:

1. Появится ссылка на Указ;

2. По факту утверждения Правительством типового положения о структурном подразделении органа (организации), обеспечивающем информационную безопасность, в состав приказа приложением будет включено положение об ответственном. Будет скорректирована инструкция ответственного;

3. Скорректированы справки к функционалу и наименования блоков/полей ввода данных.

Пункт 1, пп. в): принимать в случае необходимости решения о привлечении организаций к осуществлению мероприятий по обеспечению информационной безопасности органа (организации). При этом могут привлекаться исключительно организации, имеющие лицензии на осуществление деятельности по технической защите конфиденциальной информации.

Аналогичное требование о привлечении организаций, имеющих лицензии на осуществление деятельности по технической защите конфиденциальной информации, присутствует в следующих формируемых ПК «АльфаДок» документах:

- Положение по организации и проведению работ по обеспечению безопасности защищаемой информации при ее обработке в информационных системах;

- Положение по обеспечению безопасности значимых объектов КИИ.

Пункт 1, пп. г): принимать в случае необходимости решения о привлечении организаций к осуществлению мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты. При этом могут привлекаться

исключительно организации, являющиеся аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, за исключением случая, предусмотренного подпунктом "б" пункта 5 настоящего Указа.

Пункт 1, пп. д): обеспечивать должностным лицам органов федеральной службы безопасности беспрепятственный доступ (в том числе удаленный) к принадлежащим органам (организациям) либо используемым ими информационным ресурсам, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети "Интернет", в целях осуществления мониторинга, предусмотренного подпунктом "в" пункта 5 настоящего Указа, а также обеспечивать исполнение указаний, данных органами федеральной службы безопасности по результатам такого мониторинга

Пункт 1, пп. е): обеспечивать незамедлительную реализацию организационных и технических мер, решения о необходимости осуществления которых принимаются Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю в пределах их компетенции и направляются на регулярной основе в органы (организации) с учетом меняющихся угроз в информационной сфере

Будут внесены корректировки в следующие документы:

- Положение по организации и проведению работ по обеспечению безопасности защищаемой информации при ее обработке в информационных системах;

- Положение по обеспечению безопасности значимых объектов КИИ.

Пункт 2: возложить на руководителей органов (организаций) персональную ответственность за обеспечение информационной безопасности соответствующих органов (организаций)

Каких-либо срочных корректировок вносить не требуется. Дополнительно отразим в следующих документах:

- Положение по организации и проведению работ по обеспечению безопасности защищаемой информации при ее обработке в информационных системах;

- Положение по обеспечению безопасности значимых объектов КИИ;

- Политика обеспечения безопасности КИИ.

Пункт 3: относится к Правительству РФ и нами не рассматривается.

Пункт 4: органам (организациям), включенным в перечень, определенный в соответствии с подпунктом "б" пункта 3 настоящего Указа, осуществить мероприятия по оценке уровня защищенности своих информационных систем и до 1 июля 2022 г. представить доклад в Правительство Российской Федерации

1. Оценка уровня защищенности информационных систем может быть проведена в контексте выполнения требований приказов ФСТЭК России (№17 по ГИС, №21 по ИСПДн, №239 по ЗОКИИ) в рамках функционала «Оценка эффективности принятых мер»;

2. Оценка выполнения мер, предусмотренных приказами ФСТЭК России №21 и №17, и состояния используемых средств защиты информации в подведомственных (подконтрольных) организациях может быть выполнена в ходе формирования различных отчетов в модуле «Модуль контроля подведомственных учреждений»;

3. Оценка выполнения мер, предусмотренных приказами ФСТЭК России №21 и №17, и покрытие средствами защиты информации автоматизированных рабочих мест пользователей и серверов в организации может быть выполнена в функционале «Карточка ИС»;

4. Состояние средств защиты информации (лицензий и сертификатов ФСТЭК России и ФСБ России) может быть получено из реестра СЗИ и посредством формирования отчета в разделе «Отчеты» рабочего стола «Аналитика».

Пункт 5: относится к ФСБ России и нами не рассматривается.

Пункт 6: установить, что с 1 января 2025 г. органам (организациям) запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними.

Будут внесены корректировки в следующие документы:

- Положение по организации и проведению работ по обеспечению безопасности защищаемой информации при ее обработке в информационных системах;

- Положение по обеспечению безопасности значимых объектов КИИ.