|  |  |
| --- | --- |
|  | Приложение 8 |
|  | к Приказу Комитета финансов |
|  | Ленинградской области |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Карта рисков**

**юридически значимого электронного документооборота**

**в информационной системе «Управление бюджетным процессом**

**Ленинградской области»**

1. **Термины и сокращения**

Термины и сокращения, используемые в настоящем Регламенте, перечислены в Приложении 1 к Приказу Комитета финансов Ленинградской области \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Общие сведения**

Настоящий документ предназначен для описания вероятности возникновения рисков при использовании ЮЗЭД в Системе и мероприятий по их снижению, а также описания возможной степени причиненного ущерба.

1. **Классификация рисков**

Риски, связанные с ведением электронного документооборота в Системе, можно разделить:

 - по типу: организационные и технические;

 - по источнику возникновения: внешние и внутренние.

Классификация рисков представлена в таблицах 3 и 4.

1. **Вероятность реализации рисков, подверженность информационных активов воздействию рисков**

С целью выделения групп близких по значимости рисков и подготовки полученных материалов для дальнейшего (например, количественного) анализа для каждого риска, выявленного в процессе анализа, экспертным путем оценивались следующие показатели (присваивались значения атрибутов):

1. Вероятность реализации риска;
2. Уровень подверженности актива воздействию (существенность ущерба для Комитета финансов Ленинградской области).

Текстовые описания значений атрибутов приведены в таблицах 1 и 2.

Таблица 1. Значения атрибута «Вероятность реализации риска»

|  |  |
| --- | --- |
| Вероятность | Описание |
| Высокая | Вероятна реализация риска один или несколько раз в течение года. |
| Средняя | Риск может быть реализован хотя бы один раз в течение двух-трёх лет. |
| Низкая | Реализация риска в течение трех лет маловероятна. |

Таблица 2. Значения атрибута «Уровень подверженности актива воздействию»

|  |  |
| --- | --- |
| Уровень подверженности воздействию | Существенность ущерба(конфиденциальность/целостность актива) |
| 5 | Серьезные повреждения (например, повреждения видимые снаружи и существенно влияющие на ход производственных процессов или существенно увеличивающие затраты) или полный выход актива из строя. |
| 4 | Серьезные повреждения, не приводящие к полному выходу актива из строя (например, повреждения невидимые снаружи, но существенно влияющие на ход производственных процессов, или увеличивающие затраты). |
| 3 | Средние повреждения или ущерб (например, повреждения, влияющие на внутренние регламенты, увеличивающие затраты). |
| 2 | Незначительные повреждения или ущерб. |
| 1 | Небольшие изменения актива. |

**Таблица 3. Организационные риски**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Тип риска(Внутренний/внешний) | Описание | Вероятность реализации | Существенность ущерба | Меры по снижению риска |
|  | Внутренний/Внешний | Компрометация ключа ЭП путём хищения носителей/копирования данных | Высокая | 4 | * Организация хранения материальных носителей, журналов выдачи;
* Использование не копируемых материальных носителей.
 |
|  | Внутренний | Нарушение уполномоченным сотрудником правил использования СЭП | Высокая | 3 | Ознакомление сотрудника под роспись в журнале ознакомления с пакетом документации по ЮЗЭД. |
|  | Внутренний | Увольнение уполномоченного сотрудника, имевшего доступ к ключам ЭП | Высокая | 3 | Подача заявления в УЦ на отзыв сертификата ЭП. |
|  | Внутренний | Отказ от выполнения должностных обязанностей (в части использования электронной подписи) ввиду наличия риска компрометации ключа. | Средняя | 4 | Обучение персонала (ознакомление с нормами действующего законодательства и внутренними нормативными актами, регламентирующими применение ЭП). |
|  | Внутренний | Несоответствие Системы требованиям ФСТЭК в части защиты информации | Средняя | 5 | * Проведение аттестации Системы на 1Г;
* Обеспечение доступности информации об аттестате соответствия для всех заинтересованных в предоставлении гарантий лиц (физических и юридических).
 |
|  | Внутренний | Выгрузка в архивное хранение произведена не полностью с нарушением целостности информации о цепочках доверия или с нарушением целостности документарных томов. Утрата документов или их реквизитов в процессе выгрузки. | Высокая | 4 | * Описание регламента выгрузки документов на архивное хранение;
* Приказ о вводе в действие регламента и регламент хранения документов в архиве.
 |
|  | Внутренний | Низкая степень значимости (важности) сертификата ключа подписи как документа для уполномоченных сотрудников. | Высокая | 4 | Выдача бумажного оригинала сертификата, изготовленного на типографском бланке. |
|  | Внутренний/Внешний | Не санкционированный доступ к техническим средствам Системы (серверам, рабочим станциям уполномоченных сотрудников и т.д.) | Средняя | 5 | Организация пропускного режима в помещения, где размещены технические средства Системы, а так же в кабинеты, в которых расположены рабочие станции уполномоченных сотрудников. |
|  | Внутренний | Отказ от признания результатов экспертизы ЭД одним из участников. | Высокая | 3 | Разработка порядка разбора конфликтных ситуаций, описывающего действия при разборе конфликтных ситуаций (в т. ч. претензионный порядок разрешения конфликтов). |
|  | Внутренний | Разрешение конфликтов в суде | Средняя | 5 | Описание досудебного разбора конфликтов. |
|  | Внутренний | Длительная остановка производственного процесса по причине невозможности проведения изъятия (выемки) документов контролирующими органами (ситуация рассматривается как экстренная для Стороны) | Средняя | 5 | Описание порядка предоставления документов по запросу контролирующих органов. |
|  | Внутренний | Доступ пользователей к не принадлежащим им объектам Системы | Высокая | 3 | Использование системы разграничения прав доступа, настройка ролей пользователей. |
|  | Внутренний | Утечка персональных данных из Системы | Средняя | 3 | * Заключение соглашения о неразглашении персональных данных с физическими лицами, данные которых заносятся в Систему;
* Заключение соглашения о неразглашении с каждым пользователем Системы. В соглашение о неразглашении включить пункт «О персональных данных».
 |
|  | Внутренний | Сопротивление персонала внедрению и использованию ЮЗЭД, неприятие новых методов работы | Высокая | 4 | * Каждый этап внедрения сопровождается письменными распоряжениями руководства Комитета финансов Ленинградской области;
* Организация обучения сотрудников.
 |
|  | Внутренний | Утечка конфиденциальной информации | Высокая | 5 | Разработка внутренних нормативных актов о персональной ответственности сотрудников. |

Таблица 4. Технические риски

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Тип риска (Внутренний/внешний) | Описание | Вероятность реализации | Существенность ущерба | Меры по снижению риска |
|  | Внешний | Перехват информации, передаваемой по каналам связи | Средняя | 4 | Защита протокола передачи данных между клиентами и веб-серверами путём организации https-доступа к веб серверу, SSL-шифрование трафика между клиентами и веб серверами. |
|  | Внешний | Несанкционированный доступ к серверам Системы | Средняя | 5 | * Организация VPN сети;
* Расположение серверов в DMZ;
* Ограничение по портам доступа к серверам приложений Системы;
* Использование аппаратного брандмауэра.
 |
|  | Внутренний | Нарушение целостности данных БД | Высокая | 5 | Резервное копирование средствами используемых СУБД (средств управления базами данных). |
|  | Внутренний/Внешний | Утечка ключей ЭП с рабочих станций уполномоченных сотрудников | Средняя | 4 | Применение к рабочим станциям единой политики безопасности. |
|  | Внешний | Заражение компьютерными вирусами | Средняя | 4 | Организация антивирусной защиты. |
|  | Внутренний | Нехватка производственных мощностей серверов Системы | Низкая | 3 | Анализ планируемой нагрузки и наращивание мощностей в случае необходимости. |