**О классификации Автоматизированного рабочего места сотрудника службы по противодействию легализации доходов, полученных преступным путем» (АРМ Финансового мониторинга) как системы обработки персональных данных**

Кредитные организации при организации работ по защите информационных систем, обрабатывающих персональные данные могут использовать два пути:

1. Присоединиться в Стандарту Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации.
2. Самостоятельно классифицировать используемые информационные системы и обеспечить соответствующую защиту данных.

В первом случае **«**В соответствии с Федеральным законом от 27 декабря 2002г. № 184-ФЗ «О техническом регулировании» все стандарты носят рекомендательный характер.

Вместе с тем, в случае введения их в организации БС РФ приказом, стандарты принимают статус документов, обязательных для выполнения в этой организации. В этом случае организация БС РФ добровольно принимает на себя обязательство внедрить Стандарты Банка России, оценить соответствие организации БС РФ его требованиям (с использованием стандарта Банка России СТО БР ИББС-1.2) и официально подтвердить это, направив в адрес Банка России и территориальных органов Регуляторов – Роскомнадзора, ФСТЭК России, ФСБ России (в пределах их полномочий) «Подтверждение соответствия организации БС РФ стандарту Банка России СТО БР ИББС-1.0». 1)

В соответствии с пунктом d раздела V, СПО АРМ Финансового мониторинга ***не является ИСПДн***:

**«d. Классификация ИСПДн (пункт 6 программы действий)**

В связи с тем, что согласно статье 19 Федерального закона «О персональных данных» операторы обязаны защитить персональные данные от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий, то все ИСПДн организации БС РФ относятся к категории специальных в соответствии с пунктом 8 Порядка проведения классификации информационных систем персональных данных, утвержденного приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

**Автоматизированные системы, в которых обрабатываются персональные данные, но целью работы которых не является обработка персональных данных, включаются в перечень систем, обрабатывающих персональные данные, но не классифицируются как ИСПДн.**

По результатам классификации ИСПДн составляется Акт классификации.» 1)

Если организация БС РФ не вводит Стандарты Банка России приказом, то ее деятельность при обработке персональных данных подлежит оценке при осуществлении надзора и контроля уполномоченными государственными органами на соответствие требованиям нормативных документов Регуляторов в области персональных данных, без учета отраслевых особенностей банковской сферы деятельности, отраженных в Комплексе БР ИББС.»1)

При этом варианте действий возможно руководствоваться следующими материалами.

Правительство Российской Федерации в своих Постановлениях № 687, № 781 и № 512 возлагает на кредитные организации обязанность использовать средства и методы по обеспечению безопасности персональных данных (далее - ПДн), которые конкретизируются соответствующими Положениями и Требованиями, утвержденными этими Постановлениями, а также иными подчиненными им нормативными актами, такими как Руководящие Документы ФСБ и ФСТЭК.

Обеспечивая безопасность ПДн кредитная организация обязана руководствоваться вышеописанными постановлениями, но **она может самостоятельно определять методы и способы их обработки**. Таким образом, **кредитная организация может создавать несколько информационных систем** персональных данных (ИСПДн), **содержащих данные одних и тех же субъектов** – иными словами, она может для удобства обработки копировать персональные данные из одной ИСПДн (банковская АБС) в другую, принадлежащую ей же (АРМ Финансового мониторинга). Для каждой такой ИСПДн требуется создать систему защиты в соответствии с Постановлениями Правительства. Однако, **защита от нарушений требований**, описанных в статье 19 Федерального Закона «О персональных данных», **должна быть обеспечена с целью недопущения нанесения ущерба субъекту**. Следовательно, для **хотя бы одной** ИСПДн, содержащей все обрабатываемые кредитной организацией персональные данные, должна быть реализована защита обеспечивающая безопасность всех указанных характеристик (банковская АБС). В таком случае, **для АРМ Финансового мониторинга, содержащего некоторое подмножество всех ПДн кредитной организации, нарушение любого из требований безопасности, кроме конфиденциальности, не повлечет за собой ущерб субъекту ПДн** в смысле Закона.

Согласно совместному приказу ФСТЭК, ФСБ и Мининформсвязи от 13 февраля 2008 года № 55/86/20 по заданным кредитной организацией характеристикам безопасности персональных данных, обрабатываемых в информационной системе, информационные системы подразделяются на типовые и специальные информационные системы.

Типовые информационные системы – информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.

Специальные информационные системы – информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

К специальным информационным системам **должны** быть отнесены:

1) информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;

2) информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

Таким образом, в соответствии с Законом обеспечив безопасность персональных данных для наиболее полной ИСПДн (банковская АБС), **для АРМ Финансового мониторинга**, содержащего лишь некоторое подмножество персональных данных, определенных требованиями Федерального закона от 07.08.2001 №115-ФЗ “О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма”, кредитная организация обязана обеспечить **лишь конфиденциальность** обрабатываемых данных. Таким образом, АРМ Финансового мониторинга не попадает под два названых выше исключения, и его можно классифицировать как «типовая ИСПДн».

В соответствии с Приказом ФСТЭК, ФСБ, Мининформсвязи 13.02.08 г. № 55/86/20, АРМ Финансового мониторинга (далее – АРМ), как «типовая» ИСПДн подлежит классификации.

Классификация АРМ проводится лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных.

Классификация АРМ проводится на этапе создания или в ходе эксплуатации с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных.

Проведение классификации АРМ включает в себя следующие этапы:

* сбор и анализ исходных данных;
* присвоение АРМ соответствующего класса и его документальное оформление.

При проведении классификации АРМ учитываются следующие исходные данные:

* категория обрабатываемых персональных данных - Хпд;
* объем обрабатываемых персональных данных (количество субъектов персональных данных) - Хнпд;
* заданные оператором характеристики безопасности персональных данных;
* структура АРМ;
* наличие подключений АРМ к сетям связи общего пользования и (или) сетям международного информационного обмена;
* режим обработки персональных данных;
* режим разграничения прав доступа пользователей АРМ;
* местонахождение технических средств АРМ.

В общем случае существуют следующие категории обрабатываемых персональных данных (Хпд):

* категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
* категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
* категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;
* категория 4 - обезличенные и (или) общедоступные персональные данные.

С использованием АРМ Финансового мониторинга обрабатываются персональные данные категории ***3 -*** ***персональные данные, позволяющие идентифицировать субъекта персональных данных***.

Хпд = 3

Объем обрабатываемых персональных данных (количество субъектов персональных данных) - Хнпд может принимать следующие значения:

1. в базе данных АРМ одновременно хранятся и обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;
2. в базе данных АРМ одновременно хранятся и обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;
3. в базе данных АРМ одновременно хранятся и обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

Подавляющее большинство кредитных организаций с использованием АРМ Финансового мониторинга обрабатывает и хранит сведения о персональных данных до 100 000 клиентов, таким образом:

Хнпд = 2

Программное обеспечение АРМ в кредитной организации может использоваться в следующих вариантах:

* автономно;
* в составе комплекса автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);
* в составе комплекса автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

По режиму обработки персональных данных АРМ может быть однопользовательским или, при установке Сервера блокировок и сообщений (СБИС), многопользовательским.

В АРМ реализована функция разграничения прав доступа.

По результатам вышесказанного и в соответствии с таблицей, приведенной в Приказе ФСТЭК, ФСБ, Мининформсвязи 13.02.08 г. № 55/86/20 (табл.1), АРМ может быть присвоен класс:

* класс 3 (К3) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных.

Таблица 1. Классификация типовой ИСПДн.

|  |  |  |  |
| --- | --- | --- | --- |
| Хнпд | 3 | 2 | 1 |
| Хпд |
| Категория 4 | К4 | К4 | К4 |
| Категория 3 | К3 | К3 | К2 |
| Категория 2 | К3 | К2 | К1 |
| Категория 1 | К1 | К1 | К1 |

Результаты классификации АРМ должны быть оформлены соответствующим актом.

В соответствии с приказом ФСТЭК России от 05.02.2010 № 58, к ИСПДн ***3 класса*** защищенности должны быть применены следующие методы и способы защиты информации от несанкционированного доступа:

2.1. Для информационных систем 3 класса при однопользовательском режиме обработки персональных данных применяются следующие основные методы и способы защиты информации:

а) управление доступом:

идентификация и проверка подлинности пользователя при входе в систему информационной системы по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

***Программное обеспечение АРМ Финансового мониторинга имеет встроенную систему проверки подлинности пользователя при входе по паролю. Длина пароля, периодичность его смены устанавливается администратором АРМ при его настройке.***

б) регистрация и учет:

регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы;

***Программное обеспечение АРМ Финансового мониторинга имеет встроенную систему регистрации входа (выхода) пользователя в АРМ (выход из программы). Данные регистрации сохраняются в таблице базы данных SYSTEMEVENTSHISTORY. Расшифровка значений сохраненных событий может быть проведена с помощью таблицы базы данных EVENTS. Возможна настройка отображения таблицы SYSTEMEVENTSHISTORY для администратора АРМ.***

учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета;

в) обеспечение целостности:

обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ;

***Обеспечение целостности программных средств касается систем защиты персональных данных.***

***Целостность программной среды обеспечивается отсутствием на технических средствах пользователей программного обеспечения АРМ Финансового мониторинга средств разработки и отладки программ, интегрированных средств разработки баз данных - СУБД Access, PLSQL, Oracle и пр.***

физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;

периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;

наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

2.2. Для информационных систем 3 класса при многопользовательском режиме обработки персональных данных **и равных правах** доступа к ним пользователей применяются следующие основные методы и способы защиты информации:

а) управление доступом:

идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

***Программное обеспечение АРМ Финансового мониторинга имеет встроенную систему проверки подлинности пользователя при входе по паролю. Длина пароля, периодичность его смены устанавливается администратором АРМ при его настройке.***

б) регистрация и учет:

регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная);

***Программное обеспечение АРМ Финансового мониторинга имеет встроенную систему регистрации входа (выхода) пользователя в АРМ (выход из программы). Данные регистрации сохраняются в таблице базы данных SYSTEMEVENTSHISTORY. Расшифровка значений сохраненных событий может быть проведена с помощью таблицы базы данных EVENTS. Возможна настройка отображения таблицы SYSTEMEVENTSHISTORY для администратора АРМ.***

учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета;

в) обеспечение целостности:

обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, а целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации;

***Обеспечение целостности программных средств касается систем защиты персональных данных.***

***Целостность программной среды обеспечивается отсутствием на технических средствах пользователей программного обеспечения АРМ Финансового мониторинга средств разработки и отладки программ, интегрированных средств разработки баз данных - СУБД Access, PLSQL, Oracle и пр.***

физическая охрана информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;

периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;

наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

2.3. Для информационных систем 3 класса при многопользовательском режиме обработки персональных данных **и разных правах доступа** к ним пользователей применяются следующие основные методы и способы защиты информации:

а) управление доступом:

идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длинной не менее шести буквенно-цифровых символов;

***Программное обеспечение АРМ Финансового мониторинга имеет встроенную систему проверки подлинности пользователя при входе по паролю. Длина пароля, периодичность его смены устанавливается администратором АРМ при его настройке.***

б) регистрация и учет:

регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа;

***Программное обеспечение АРМ Финансового мониторинга имеет встроенную систему регистрации входа (выхода) пользователя в АРМ (выход из программы). Данные регистрации сохраняются в таблице базы данных SYSTEMEVENTSHISTORY. Расшифровка значений сохраненных событий может быть проведена с помощью таблицы базы данных EVENTS. Возможна настройка отображения таблицы SYSTEMEVENTSHISTORY для администратора АРМ.***

учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);

в) обеспечение целостности:

обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

***Обеспечение целостности программных средств касается систем защиты персональных данных.***

***Целостность программной среды обеспечивается использованием транслятора языка JAVA и отсутствием на технических средствах пользователей программного обеспечения АРМ Финансового мониторинга средств разработки и отладки программ, интегрированных средств разработки баз данных - СУБД Access, PLSQL, Oracle и пр.***

физическая охрана информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;

периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;

наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонент средств защиты информации, их периодическое обновление и контроль работоспособности.

***Остальные методы и способы защиты ПДн реализуются организационными и техническими мероприятиями, проводимыми кредитной организацией и напрямую не касаются программного обеспечения АРМ Финансового мониторинга.***

**Вывод:**

**АРМ Финансового мониторинга, при выполнении организационно-технических мероприятий, соответствует требованиям защищенности персональных данных по классу 3 для многопользовательского режима с разными правами доступа к данным.**

*Использованные материалы:*

*1. Методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях банковской системы Российской Федерации. Банк России. Ассоциация российских банков. Ассоциация региональных банков России (Ассоциация «РОССИЯ»), 2010г.*

*2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».*

*3. Федеральный закон Российской Федерации от 13 июля 2001 г. «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».*

*4. Приказ ФСТЭК от 5 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».*

*5. Приказ ФСТЭК, ФСБ, Мининформсвязи 13.02.08 г. N 55/86/20.*