С.В. Сомов, В.М. Шаймарданов

О ЗАЩИТЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ В ФОНДЕ ДАННЫХ РОСГИДРОМЕТА

S.V. Somov, V.M. Shaimardanov

ON PROTECTION OF INFORMATION RESOURCES OF ROSHYDROMET DATA FUND

Рассматривается системный подход к организации обеспечения защиты данных хранящихся в автоматизированной системе (АС) Единого государственного фонда данных (ЕГФД) по окружающей среде и ее загрязнению в соответствии с требованиями законодательства РФ. На основе анализа АС ЕГФД выделены и классифицированы основные источники угроз безопасности информационных ресурсов, проведена оценка вероятности их реализации, так же определен перечень основных мероприятий и средства противодействия этим угрозам.

Ключевые слова: данные. Информационные ресуры. Защита информации. Единый государственный фонда данных (ЕГФД).

A systematic approach is considered to the organization of data protection on the Automated System of the Unified State Fund of Data on the Environment and Environmental Pollution (according to the requirements of the Russian Federation Legislation. Based on the analysis of the Automated System of the Unified State Fund of Data on the Environment and Environmental Pollution, the main sources of threats to information resources security have been determined and classified; the threat probability has been assessed and also the list of major activities and threat response means have been identified.

Keywords: data, information resources, protection of Information, unified State Fund of Data.

Информационные ресурсы в области гидрометеорологии и смежных с ней областях, хранящиеся в Едином государственном фонде данных (ЕГФД) Росгидромета, относятся к государственным информационным ресурсам и в соответствии с законодательством РФ подлежат защите [1]. Основой современной доктрины информационной безопасности является обеспечение интересов всех субъектов информационных отношений, которые заключаются в законном праве их доступа и получения достоверной информации за приемлемое время, а в некоторых случаях, предусмотренных законом, и в сохранении ее конфиденциальности.

Особую специфику проблема защиты приобретает в связи с тем, что в современном обществе, в том числе и в гидрометеорологии, средой обработки данных и местом ее долговременного хранения являются специализированные центры, где сосредоточены мощные средства вычислительной техники, роботизированные библиотеки и информационно-телекоммуникационная инфраструктура. Специалисты таких центров наравне с другими субъектами информационных отношений (наблюдателями, потребителями), также заинтересованы в ми-

нимизации возможного ущерба от потери и искажения данных, которые могут возникнуть в результате нештатной работы программных и технических средств и ряда других угроз, так как всё это может привести к компрометации информации: нарушению её целостности, конфиденциальности и доступности [2]. К числу таких центров, содержащих информацию в области гидрометеорологии и смежных с ней областях, относится и ЕГФД по окружающей среде и ее загрязнению, ведение которого возложено на ГУ «ВНИИГМИ-МЦД».

Под доступностью информации в ЕГФД понимается законное право субъектов информационных отношений получать доступ к имеющимся в фонде данным и сведениям за приемлемое время. Средства защиты информации для реализации права доступа должны быть направлены против угроз блокирования и/или уничтожения информации, а критерием эффективности защиты является время доступа к информации. Обеспечение права субъектов в получении достоверной информации в ЕГФД сводится к защите и контролю целостности хранящихся в ней данных и сведений, т.е. предотвращению угроз несанкционированной модификации гидрометеорологических и других данных фонда и их соответствия первоисточнику. Законное право сохранения в тайне некоторой части информации должно быть реализовано при помощи средств защиты направленных на предотвращение угроз несанкционированного доступа (НСД) к информационным ресурсам. Таким образом, три компоненты: доступность, целостность и конфиденциальность информации представляют собой суть системного подхода к ее защите в ЕГФД. Каждая из этих компонент должна быть обеспечена специфической совокупностью мер и средств защиты. Для их определения необходимо провести анализ угроз информационной безопасности, оценить вероятность их реализации и комплекс организационных мер и программно-технических средств защиты.

Автоматизированная система (АС) ЕГФД, которая призвана решать задачи автоматизации процессов комплектования, ведения фонда и обслуживания потребителей, представляет собой совокупность, специальным образом организованных, коллекций данных (массивов, баз данных) на электронных носителях, технических и программных средств их сбора, обработки, долговременного хранения, информационного обслуживания и обмена с другими системами. Она также включает в себя и персонал, принимающий участие как в технологических заданиях, так и в обеспечении работоспособности АС.

На основе анализа АС ЕГФД нами выделены следующие основные источники угроз безопасности информационных ресурсов:

1. Непреднамеренные угрозы.

Источником непреднамеренных угроз, как правило, являются пользователи, операторы, системные администраторы и другие сотрудники ГУ «ВНИИГМИ-МЦД», обслуживающие систему, т.е. они являются внутренними источниками случайных воздействий, т.к. имеют непосредственный доступ к процессам обработки информации и могут совершать непреднамеренные ошибки.

2. Преднамеренные угрозы несанкционированного доступа к информации (НСД).

Угрозы представляют собой основные возможные пути умышленной дезорганизации работы, вывода АС ЕГФД из строя, проникновения в систему и несанкционированного доступа к информации (с корыстными целями, по принуждению, из желания отомстить и т.п.). К ним нами отнесены:

- угрозы уничтожения или хищения аппаратных средств, носителей информации *путем физического доступа к элементам АС ЕГФД;*
- угрозы утечки, несанкционированной модификации или блокирования информации *с применением программно-аппаратных или программных средств;*
- угрозы преднамеренных действий *внутренних нарушителей*;
- угрозы несанкционированного доступа к АС ЕГФД *по каналам связи*;

Оценка вероятности реализации угроз проводилась экспертно на основе качественных показателей по шкале, где:

0 < X < 0,25 – низкая вероятность реализации угрозы;

0,25 <= X <= 0,5 – средняя;

0,5 < X < 0,75 – высокая;

0,75 <= X < 1,0 – очень высокая.

Все выделенные нами угрозы и полученные оценки вероятности их реализации в АС ЕГФД, а также перечень основных мероприятий и средства противодействия угрозам сведены в табличный вид (табл. 1 и 2).

Из таблиц видно, что наименьшее количество угроз (6) у нас попадает в группу с высокой вероятностью их реализации, а больше всего угроз (12) попадает в группу с низкой вероятностью реализации. В группу со средней вероятностью реализации попало 11 угроз, что только на единицу меньше чем угроз с низкой вероятностью. То есть по мере роста вероятности реализации угроз их количество уменьшается.

Ранжируя угрозы, по оценкам вероятности их реализации, видно, что наибольшее число угроз (4), представляющих высокую опасность информационным ресурсам, попадает в класс «Непреднамеренные угрозы», а в классе «Преднамеренные угрозы» их только 2. При этом одну из двух преднамеренных угроз представляет собой угроза несанкционированной установки на ПЭВМ или сервер АС ЕГФД программного обеспечения, не связанного с выполнением основных технологических операций сотрудником на данном АРМ. По всей видимости, такая угроза в большей степени обусловлена халатностью, возможно, даже сознательным нарушением своих должностных обязанностей, чем злым умыслом. Распределение непреднамеренных и преднамеренных угроз по группам со средней и низкой вероятностью реализации угроз произошло практически в равном отношении. Следует, правда, отметить, что число преднамеренных, умышленных угроз в этих группах в количественном отношении преобладает над непреднамеренными угрозами, т.е. риски от их реализации повышаются.

Таблица 1

Угрозы безопасности информации в Автоматизированной системе ЕГФД. Основные непреднамеренные угрозы в АС ЕГФД

Наименование угрозы	Вероятность реализации угрозы	Меры по противодействию угрозе	
		технические	организационные
1	2	3	4
Утрата атрибутов разграничения доступа (паролей, ключей шифрования или ЭЦП, идентификационных карточек, пропусков)	**низкая**	Идентификация и аутентификация. Аудит доступа	Регламент доступа и ведения атрибутов разграничения доступа. Персональная ответственность
Непреднамеренное отключение средств защиты	**низкая**	Система защиты от НСД и ее настройка. Администрирование привилегий, роли	Инструкция пользователя. Обучение персонала. Введение запретов, усиление ответственности
Неумышленная порча оборудования, отключение оборудования или изменение режимов работы устройств	**низкая**	Резервирование оборудования	Инструкция пользователя. Технологический процесс. Обучение персонала. Введение запретов, усиление ответственности
Случайное удаление, искажение программ или файлов с важной информацией (в том числе системных)	**высокая**	Администрирование привилегий, роли. Контроль целостности файлов. Резервное копирование	Инструкция пользователя. Обучение персонала. Введение запретов, усиление ответственности
Несанкционированный запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы	**средняя**	Администрирование привилегий, роли	Инструкция пользователя. Технологический процесс. Обучение персонала. Введение запретов, усиление ответственности
Неумышленная порча носителей информации	**низкая**		Инструкция пользователя. Резервирование. Обучение персонала. Введение запретов, усиление ответственности
Повреждение каналов связи	**низкая**		Инструкция пользователя Резервирование. Обучение персонала. Введение запретов, усиление ответственности
Непреднамеренное заражение компьютера вирусами	**высокая**	Антивирусная программа	Инструкция пользователя. Технологический процесс. Обучение персонала. Введение запретов, усиление ответственности

Окончание табл. 1

1	2	3	4
Ввод ошибочных данных	**высокая**	Механизмы СУБД (ограничения целостности, триггеры)	Инструкция пользователя. Обучение персонала
Другие неумышленные действия сотрудников, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств	**высокая**		Инструкция пользователя. Обучение персонала. Введение запретов, усиление ответственности
Сбои в программном обеспечении	**средняя**	Резервная копия	Инструкция пользователя
Сбои в работе аппаратных средств, в электропитании	**средняя**	Генераторы и источники бесперебойного питания. Резервирование.	Инструкция пользователя
Потеря информации или работоспособности АС ЕГФД в результате стихийных бедствий или явлений (удар молнии, пожаров, наводнений и т.д.).	**средняя**	Противопожарная сигнализация. Противопожарные средства. Громоотвод, заземление	Инструкция пользователя. Резервирование

Таблица 2

Угрозы безопасности информации в Автоматизированной системе ЕГФД.
Преднамеренные угрозы несанкционированного доступа к информации в АС ЕГФД

Наименование угрозы	Вероятность реализации угрозы	Меры по противодействию угрозе	
		технические	организационные
1	2	3	4
Угрозы уничтожения, хищения аппаратных средств, носителей информации ***путем физического доступа к элементам АС ЕГФД***			
Кража ПЭВМ или других отдельных элементов АС ЕГФД	**средняя**	Применение физических средств защиты: охранная сигнализация, видеонаблюдение, решетки на окна, металлическая дверь, кодовый замок. Шифрование данных	Пропускной режим. Охрана. Акт установки средств защиты
Кража носителей информации	**средняя**	Применение физических средств защиты: охранная сигнализация, видеонаблюдение, решетки на окна, металлическая дверь, кодовый замок. Шифрование данных	Акт установки средств защиты Учет носителей информации

Продолжение табл. 2

1	2	3	4
Умышленный вывод из строя узлов АС: ПЭВМ, серверов, каналов связи	**низкая**	Применение физических средств защиты: охранная сигнализация, видеонаблюдение, решетки на окна, металлическая дверь, кодовый замок. Программная система защиты от НСД. Резервирование	Акт установки средств защиты. Учет носителей информации и оборудования
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	**низкая**	Идентификация и аутентификация. Аудит доступа. Шифрование данных	Усиление контроля и ответственности. Регистрация действий персонала
Несанкционированное отключение средств защиты	**низкая**	Идентификация и аутентификация. Аудит доступа. Шифрование данных. Регистрация действий персонала	Акт установки средств защиты. Усиление контроля и ответственности
Угрозы утечки, несанкционированной модификации или блокирования информации *с применением программно-аппаратных или программных средств*			
Незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность сотрудников, путем подбора, путем имитации интерфейса системы программными закладками и т.д.) с последующей маскировкой под зарегистрированного пользователя	**средняя**	Средства, препятствующие внедрению программ перехвата паролей, ключей и других реквизитов. Криптографическая защита передаваемой информации	Инструкция пользователя. Обучение персонала. Введение запретов, усиление ответственности
Модификация, уничтожение информации или ее кража путем копирования.	**высокая**	Идентификация и аутентификация. Администрирование привилегий, роли. Контроль целостности файлов. Аудит доступа и действий пользователей. Резервное копирование	Акт установки средств защиты. Инструкция пользователя. Обучение персонала. Введение запретов, усиление ответственности

Продолжение табл. 2

1	2	3	4
Компьютерные вирусы	**высокая**	Антивирусное ПО	Акт установки средств защиты. Инструкция пользователя. Обучение персонала. Введение запретов, усиление ответственности
Недекларированные возможности ПО в том числе системного	**низкая**	Сертификация ПО	Документ о сертификации соответствия
Установка ПО, не связанного с исполнением служебных обязанностей (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения сотрудниками своих служебных обязанностей)	**высокая**	Администрирование привилегий, роли. Контроль целостности системы	Введение запретов, усиление ответственности
Наличие аппаратных закладок в приобретаемых ПЭВМ или другом оборудовании АС ЕГФД	**низкая**	Сертификация ПЭВМ. Настройка средств защиты	Документ о сертификации соответствия
Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями)	**низкая**		Контроль действий. Введение запретов, усиление ответственности
Угрозы преднамеренных действий внутренних нарушителей			
Несанкционированное копирование, модификация, уничтожение информации сотрудниками, не допущенными к ее обработке	**средняя**	Идентификация и аутентификация. Аудит доступа. Администрирование привилегий, роли. Контроль целостности файлов	Акт установки средств защиты. Разрешительная система допуска. Технологический процесс обработки. Введение запретов, усиление ответственности

Окончание табл. 2

1	2	3	4
Угрозы несанкционированного доступа по каналам связи			
Несанкционированный доступ к информационным ресурсам ЕГФД через ЛВС организации	**средняя**	Межсетевой экран	Технологический процесс. Инструкция пользователя. Инструкция администратора безопасности. Акт установки средств защиты
Утечка атрибутов доступа	**средняя**	Межсетевой экран	Технологический процесс. Инструкция пользователя. Инструкция администратора безопасности. Акт установки средств защиты
Перехват данных, передаваемых по каналам связи, и их анализ с целью получения конфиденциальной информации	**низкая**	Шифрование данных.	Инструкция пользователя. Инструкция администратора безопасности. Акт установки средств защиты

Технические средства защиты для противодействия таким угрозам, как видно из таблиц, включают, прежде всего, средства ограничения доступа пользователей к информационным ресурсам на основе механизмов идентификации и аутентификации пользователей, администрирования привилегий, предоставляемых пользователям на право чтения, записи, модификации и удаления каждого конкретного информационного объекта хранения, а также аудита деятельности пользователей. Кроме того, она включает средства фиксации исходного состояния и контроля целостности файлов в фонде, а также средств ограничений целостности в СУБД, применяемых на этапах обработки данных и обслуживания в технологиях АС ЕГФД. И, наконец, резервирование информационных ресурсов (в том числе и оборудования) во многих случаях является самым эффективным средством, обеспечивающим информационную безопасность.

Разработка требований к этим средствам защиты является актуальной задачей, которую необходимо дифференцированно решить на основе категорирования информационных ресурсов в области гидрометеорологии и смежных с ней областях. Прежде всего, это относится к информации, ограничения на распространение которой могут быть введены руководством организации в соответствии с предоставленными действующим законодательством правами. Кроме того, требования к средствам защиты зависят от категорирования данных и сведе-

ний по уровню допустимой задержки в получении информационных ресурсов, от уровня, когда задержка получения не должна превышать нескольких минут, до уровня, когда временные задержки для доступа не лимитированы. По аналогии, необходимо осуществить категорирование информационных ресурсов ЕГФД по уровню защиты целостности и аутентичности данных и сведений, а каждая из категорий также должна быть обеспечена гарантированными методами защиты.

Другой, не менее эффективный, способ защиты данных обеспечивается организационными мерами противодействия угрозам в АС ЕГФД. Организационные меры защиты – это, прежде всего, меры, регламентирующие процессы функционирования систем обработки данных, использование их ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации. К таким мерам нами отнесены регламентации:

- доступа в помещения (в здание, на территорию);
- допуска сотрудников к использованию информационных ресурсов, регламентация процессов ведения баз данных и осуществления модификации информационных ресурсов;
- процессов обслуживания и осуществления модификации аппаратных и программных ресурсов, обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов;
- кадровая работа по обеспечению защиты информации (подбор и подготовка персонала, обучение пользователей);
- введение запретов и ответственность за нарушения установленного порядка.

Выводы

1. Классификация и оценка вероятности угроз безопасности информационных ресурсов АС ЕГФД позволила их систематизировать, определить перечень необходимых мер противодействия угрозам безопасности и расставить основные приоритеты по их эффективному применению.

2. Показана необходимость категорирования информационных ресурсов фонда с целью осуществления дифференцированного подхода для разработки требований по применению средств защиты в АС ЕГФД.

3. Предложенная совокупность организационных и технических мер противодействия угрозам позволяют минимизировать риски нарушения информационной безопасности ресурсов АС ЕГФД, построить систему ее защиты, соответствующую требованиям основных нормативных документов.

Литература

1. Федеральный закон Российской Федерации «Об информации, информационных технологиях и защите информации» № 149-ФЗ от 27.07.06 г.
2. *Сомов С.В., Шаймарданов В.М.* О защите информационных ресурсов в области гидрометеорологии и смежных с ней областях // Труды ВНИИГМИ-МЦД, 2010, вып. 174, с. 23-27.