КЛАССИФИКАЦИЯ НАРУШИТЕЛЕЙ И УГРОЗ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ УПРАВЛЯЮЩЕЙ СИСТЕМЫ МЧС РОССИИ

А.Ю. Иванов, доктор технических наук, профессор.
Санкт-Петербургский университет ГПС МЧС России.
М.Ю. Синещук. Северо-Западный региональный центр МЧС России

Проанализированы особенности организации функционирования информационных систем. Рассмотрены основные категории нарушителей безопасности и возможные угрозы, сформулирована задача снижения рисков, связанных с несанкционированной деятельностью в распределенных вычислительных сетях МЧС России на основе анализа видов деятельности пользователей и классификации сетевого трафика.

Ключевые слова: автоматизированная система управления МЧС России, распределенные вычислительные сети, нарушитель безопасности, угрозы, риск, безопасность

CLASSIFICATION OF OFFENDERS AND SECURITY THREATS AIUS OF THE MINISTRY OF EMERGENCY SITUATIONS OF RUSSIA

A.Yu. Ivanov. Saint-Petersburg university of State fire service of EMERCOM of Russia.
M.Yu. Sineshchuk. Northwest regional center of EMERCOM of Russia

The article analyses the peculiarities of the organization of functioning of information systems. Discuss the main categories of offenders security and possible threats, the task is formulated to reduce the risks of unauthorized activities in distributed computing networks of EMERCOM of Russia, based on the analysis of users activities and classification of network traffic.

Keywords: automated control system of EMERCOM of Russia, distributed computing network, intruder security, threats, risk, safety

Информационное обеспечение в единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций (РСЧС) осуществляется с использованием автоматизированной информационно-управляющей системы (АИУС) РСЧС, представляющей собой совокупность технических систем, средств связи и оповещения, автоматизации и информационных ресурсов, обеспечивающей обмен данными, подготовку, сбор, хранение, обработку, анализ и передачу информации.

АИУС предназначена для информатизации и автоматизации деятельности органов управления РСЧС по предупреждению и ликвидации ЧС, выполнению мероприятий гражданской обороны на федеральном, региональном, территориальном, местном и объектовом уровнях [1].

Учитывая специфику МЧС России как координатора, обеспечивающего взаимодействие органов государственного управления при решении задач в условиях чрезвычайных ситуаций, АИУС РСЧС должна занимать центральное место, объединяя информационные ресурсы автоматизированных систем МЧС России, осуществляющих сбор информации на всей территории Российской Федерации.

Распределенные вычислительные сети (РВС) являются материальной (технической) основой реализации АИУС РСЧС. Они представляют собой сложные системы,

предназначенные для обработки, хранения и передачи информации, поэтому вопросы обеспечения безопасности в вычислительных сетях требуют особого внимания [2].

Несомненные преимущества обработки информации в распределенных вычислительных сетях оборачиваются немалыми сложностями при организации их защиты. Отметим следующие основные проблемы:

– расширение зоны контроля;
– комбинация различных программно-аппаратных средств;
– неизвестный периметр;
– множество точек атаки;
– сложность управления и контроля доступа к РВС МЧС России.

Для выработки мер обеспечения безопасности в распределенных вычислительных сетях необходимо провести общую классификацию информационных угроз [3, 4]. Проведение классификации играет важную роль при оценке реально существующих угроз для конкретных реализаций распределенных вычислительных сетей (рис. 1).

Данная классификация показывает, что количество возможных внутренних угроз значительно превышает количество внешних. И даже случай с воздействием злоумышленников на персонал является внутренним источником угроз безопасности РВС МЧС России. Внутренние угрозы практически полностью связаны с пользователями вычислительных сетей.

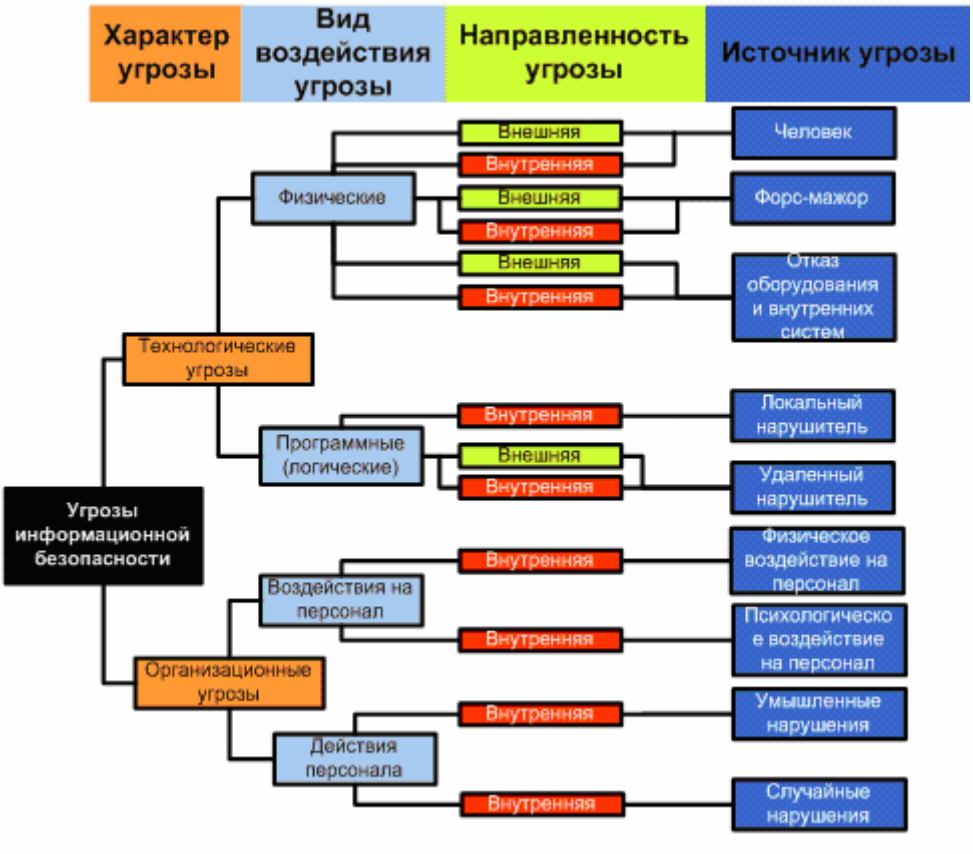

Рис. 1. **Классификация информационных угроз по направленности**

Обобщенный состав наиболее опасных внутренних угроз нарушения безопасности информации в РВС представлен на рис. 2

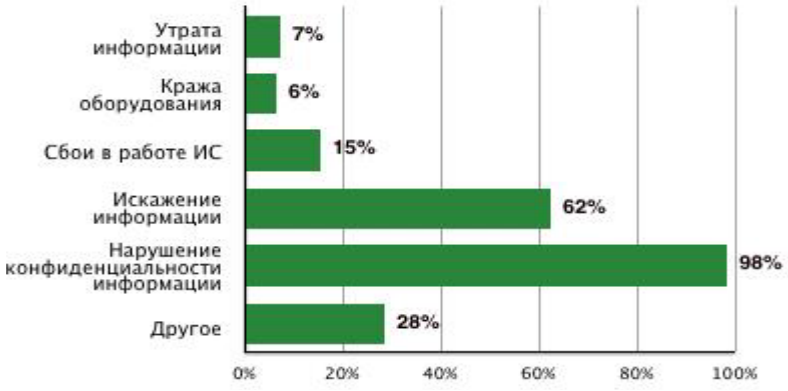

Рис. 2. **Наиболее опасные внутренние угрозы безопасности информации**

Вместе с тем анализ существующих средств и методов защиты информации показывает, что подавляющее большинство решений, обеспечивающих информационную безопасность РВС, предлагают защиту данных исключительно от внешних угроз. На другую сторону безопасности, в которой сосредоточены угрозы внутренние, как правило, не обращают внимания, основываясь на предположении об идеальной честности и профессиональной компетенции пользователей.

При разработке мер безопасности необходимо рассматривать все возможные для данной организации категории нарушителей, которых можно классифицировать следующим образом (табл.).

Таблица. **Классификация нарушителей информационной безопасности**

Внешние нарушители	Внутренние нарушители
Конкуренты	Администраторы
Клиенты (представители сторонних организаций, граждане)	Сотрудники отделов разработки и сопровождения ПО (прикладные и системные программисты)
Посетители	Пользователи (операторы) системы
Хакеры	Руководители различных уровней должностной иерархии
Преступные организации	Технический персонал

Согласно исследованиям Агентства CNews Analytics (CNA) наиболее серьёзными угрозами информационной безопасности компаний были названы планомерная утечка информации (73 %) и халатность персонала, допустившего утечку данных (70 %).

Односторонность современных систем безопасности связана с тем, что внутренние проблемы значительно труднее внешних. Практика показывает, что действия собственных сотрудников крайне непредсказуемы, а возможностей несанкционированного доступа или хищения данных у них значительно больше, чем у внешних злоумышленников. А если возможности сотрудников ограничить слишком грубо, то работа системы может просто остановиться. Внутренняя безопасность – это всегда компромисс между организационными и техническими методами, стремлением к защищенности и потребностями рядовых пользователей. И в тоже время это непрерывный процесс, который подразумевает не только внедрение и настройку программных решений, а также работу и обучение сотрудников. Полностью защититься от внутренних угроз нельзя, но нужно стараться минимизировать риски их реализации.

Внутренний нарушитель представляет собой легитимного сотрудника организации, который обладает определенными правами на доступ к информационным ресурсам. Вследствие умышленных или ошибочных действий внутренний нарушитель может принести ущерб, зачастую больший, чем внешний злоумышленник.

Существует несколько подходов к классификации внутренних нарушителей. Один из первых шагов в этом направлении сделала компания IDC – поставщик исследований и организатор конференций в области информационных технологий. По версии IDC, экосистема внутренних нарушителей имеет четыре уровня:

– граждане – лояльные служащие, которые очень редко (если вообще когда-нибудь) нарушают корпоративную политику и в основном не являются угрозой безопасности;

– нарушители – составляют большую часть служащих организации. Эти сотрудники позволяют себе небольшие фамильярности, работают с персональной веб-почтой, играют в компьютерные игры и т.д.;

– отступники – работники, которые проводят большую часть дня, делая то, что они делать не должны. Эти служащие злоупотребляют своими привилегиями по доступу к интернету, самовольно устанавливают и используют P2P-клиенты и FTP-серверы. Более того, такие сотрудники могут отсылать конфиденциальную информацию компании внешним адресатам, заинтересованным в ней. Таким образом, «отступники» представляют серьезную угрозу безопасности информации;

– предатели – служащие, умышленно и регулярно подвергающие конфиденциальную информацию компании опасности. Обычно за финансовое вознаграждение от заинтересованной стороны. Такие сотрудники представляют самую большую угрозу, их сложнее всего поймать.

Защита от внутренних угроз с каждым годом становится все большей проблемой. В общем случае требования и рекомендации по защите информации предусматривают, что:

– обеспечение защиты информации достигается комплексным применением мер и средств защиты информации от несанкционированного доступа (НСД) к ней;

– необходим постоянный комплексный контроль за эксплуатацией средств вычислительной техники.

Такие требования не голословны, а выработаны практикой. Подобные формулировки содержатся и в британском стандарте BS 7799 «Практические правила управления информационной безопасностью», в германском стандарте BSI и в стандартах других стран.

В качестве примера распределенной вычислительной сети МЧС России рассмотрим автоматизированную систему «Делопроизводство» (АСД). Эта система является распределенной автоматизированной системой и предназначена для подготовки, обработки, хранения, документирования и доставки электронных документов и информационных массивов между объектами МЧС России, а также для обмена информацией в электронном виде с другими ведомствами. Обобщенная структура такого рода системы представлена на рис. 3.

Технической основой АСД МЧС России являются комплексы средств телекоммуникации (СТК), разворачиваемые на объектах и соединяемые между собой закрытыми каналами связи.

АСД предоставляет должностным лицам услуги по обмену информацией в двух режимах: документальный обмен, информационный обмен.

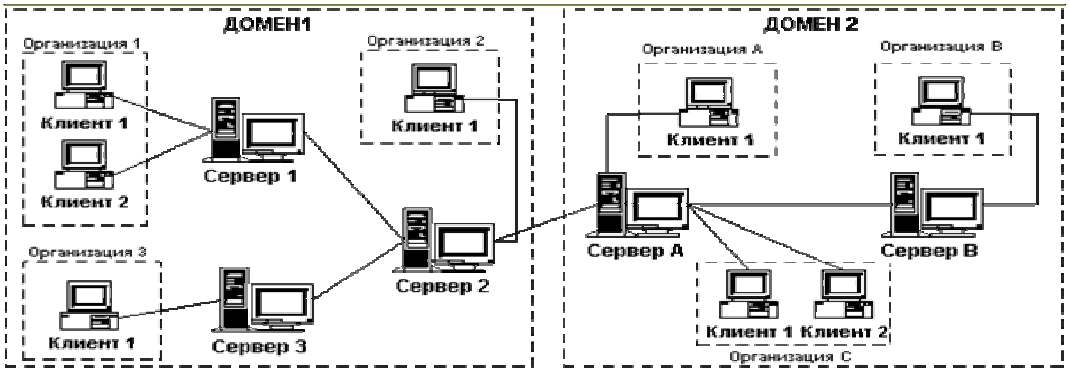

Рис. 3. **Структура АСД МЧС России**

Документальный обмен информацией различных уровней конфиденциальности может осуществляться между автоматизированными рабочими местами подразделений органов управления и отдельных должностных лиц органов управления.

Информационный обмен может осуществляться между любыми средствами вычислительной техники из состава СТК либо подключенных к СТК локальных сетей.

Базовым принципом построения АСД является такое объединение независимых сетей (подсетей), которое с точки зрения пользователя функционирует как одна большая интерсеть. АСД функционирует на базе протоколов Ethernet с использованием ОС, поддерживающих стек протоколов TCP/IP.

По взаимной локализации объекта угрозы и нарушителя будем выделять внешних и локальных нарушителей. Внешние нарушители – это пользователи и обслуживающий персонал внешних локальных вычислительных сетей (ЛВС), а также пользователи и обслуживающий персонал СТК взаимодействующих объектов. Локальные нарушители – это пользователи (операторы экспедиции) данного объекта.

По степени ограничений использования технических и программных средств доступа в АСД выделяются следующие группы нарушителей:

– Нарушители замкнутой функциональной среды (ЗФС) – должностные лица (ДЛ), допущенные к средствам доступа в АСД с ограниченным набором возможностей, определяемым характером решаемых задач. Для нарушителей ЗФС действует разрешительная политика – «что не разрешено явно, то запрещено».

– Нарушители открытой функциональной среды (ОФС) – ДЛ, допущенные к средствам доступа в АСД с возможностью запускать произвольные программы и использовать произвольные протоколы. Для нарушителей ОФС действуют запретительная политика – «что не запрещено явно, то разрешено».

– Нарушители недоверенной функциональной среды (НФС) – не предполагают использования в системе средств защиты информации и организационных мероприятий по обеспечению безопасности информации (ОБИ), требуемых для обработки конфиденциальной информации.

Для реализации НСД нарушителями ЗФС могут быть использованы следующие возможности:

– физическое воздействие на средства доступа в АСД и носителям информации (съемным и стационарным) в процессе работы;

– использование на средствах доступа в АСД программ обработки информации из ограниченного перечня, установленного инженером по ОБИ;

– взаимодействие в АСД с использованием заданных прикладных протоколов и форматов сетевых сообщений.

Модель нарушителей ЗФС допускается для внешних и локальных нарушителей без ограничения на гриф секретности информации и режима использования АСД.

Для реализации НСД, нарушители ОФС, в дополнение к возможностям нарушителей ЗФС, могут использовать:

– средства разработки и отладки программ в средствах доступа в АСД, а также возможность самостоятельно устанавливать и использовать программное обеспечение;

– взаимодействие с использованием произвольных прикладных протоколов и форматов данных (документов).

Модель нарушителя ОФС допускается для обслуживающего персонала, а также для абонентских пунктов АСД внешних ЛВС при условии использования его только для информационного обмена без ограничения на гриф обрабатываемой информации.

Нарушители НФС в дополнение к возможностям нарушителей ОФС могут использовать средства доступа в АСД, включающие в свой состав недоверенное программное обеспечение. Модель нарушителя НФС допустима для обработки только открытой информации.

Под средствами доступа в АСД понимаются вычислительные средства и программное обеспечение СТК и внешних ЛВС, с которых предоставляется доступ в АСД МЧС России.

Таким образом, в АИУС РСЧС подвергаться информационным атакам могут: глобальная сеть информационного обмена, локальные сети органов управления и отдельные компьютеры. В связи с этим для защиты информационных ресурсов МЧС России необходим комплексный подход к обеспечению информационной безопасности. Для успешного решения этой задачи необходимо развитие в АИУС РСЧС подсистемы обеспечения безопасности информации и разработка продуманной долгосрочной политики информационной безопасности, обеспечивающей защиту информации в соответствии с требованиями российского законодательства и РД ФСТЭК (Гостехкомиссии).

На подсистему обеспечения безопасности информации возлагаются задачи по организации защиты и предотвращению ущерба, который может быть нанесен государству за счет хищения, разглашения, утечки, утраты, искажения и уничтожения информации, нарушения работы технических средств, общего и прикладного программного обеспечения информационных систем АИУС РСЧС.

В соответствии с российским законодательством автоматизированные системы, обрабатывающие сведения ограниченного доступа, должны выполняться в защищенном исполнении и обеспечивать уровень защиты информации, соответствующий степени ее конфиденциальности [5]. Также требует защиты и открытая документированная информация, находящаяся в ведении МЧС России, являющаяся государственным информационным ресурсом. Поэтому защита конфиденциальности, целостности и доступности информационных, вычислительных и коммуникационных ресурсов АИУС РСЧС является обязательной и жизненно необходимой государственной задачей. Важной составной частью этой задачи является снижение рисков, связанных с несанкционированной деятельностью в распределенных вычислительных сетях МЧС России на основе анализа видов деятельности и классификации сетевого трафика.

Литература

1. Об утверждении Положения о системе и порядке информационного обмена в рамках единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций: Приказ Министерства Рос. Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий от 26 авг. 2009 г. № 496.Доступ из справ.-правовой системы «КонсультантПлюс».

2. Малыгин И.Г., Козьмовский Д.В. Методы обеспечения безопасности распределенных информационных систем МЧС России, основаннных на анализе трафика и контроле сетевой деятельности пользователей // Проблемы упр. рисками в техносфере. 2013. № 2 (26). С. 78–82.

3. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. заместителем директора ФСТЭК России 14 февр. 2008 г.) // ФСТЭК России. URL: http://fstec.ru/ (дата обращения: 15.09.2013).

4. Информационная безопасность открытых систем: в 2-х т. / С.В. Запечников [и др.]. в 2-х т. Т. 1. М.: Горячая Линия–Телеком, 2006.

5. Основные угрозы и направления обеспечения безопасности единого информационного пространства / Ю.И. Синещук [и др.] // Вестн. С.-Петерб. ун-та МВД России. 2013. № 2. С. 150–154.