Л. А. Шивдяков (к. воен. н., академик)
ФСТЭК России, г. Хабаровск

ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

В статье изложен опыт проведения проверок организации и функционирования государственной системы защиты информации в Дальневосточном федеральном округе.

В последнее время немногие из прикладных отраслей общественной деятельности развиваются столь бурно, как обеспечение информационной безопасности. Приходит осознание того, что с развитием информационных технологий возникают и стремительно растут риски, связанные с их использованием, появляются совершенно новые угрозы, с которыми человечество раньше не сталкивалось. Все чаще и чаще в средствах массовой информации отмечаются факты утечки сведений различных категорий, связанные с обострением конкурентной борьбы и криминальной обстановки.

В ходе проведенных проверок различных организаций по соблюдению установленных правил обработки, накопления, хранения и передачи сведений конфиденциального характера у проверяемых возникало множество вопросов к сотрудникам Управления ФСТЭК России по Дальневосточному федеральному округу, основным из которых являлся «порядок оценки соответствия фактического состояния защиты конфиденциальной информации, обрабатываемой в автоматизированных системах (АС), требованиям нормативно-методических документов». В этой статье, основываясь на полученном опыте проведения проверок, хотелось бы дать наиболее полный ответ на данный вопрос.

Для оценки состояния защиты конфиденциальной информации, обрабатываемой в АС, необходимы следующие документы:

«Положение о ГСЗИ», утвержденное Постановлением Правительства Российской Федерации от 15 сентября 1993 г. № 912-51;

Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Об утверждении положения о Федеральной службе по техническому и экспортному контролю»;

Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня конфиденциальной информации»;

Указ Президента Российской Федерации от 19 мая 2004 г. № 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена» (в редакции Указов Президента РФ от 22 марта 2005 г. № 329, от 3 марта 2006 г. № 175);

«Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К), утвержденные приказом Гостехкомиссии России от 30 августа 2002 г. № 282-дсп;

Сборник руководящих документов по защите информации от несанкционированного доступа, 1998 г.;

Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам, 2002 г.

При этом требования нормативных документов условно можно разбить на две основные части:

1. Требования к работам по защите информации, обрабатываемой в АС, от несанкционированного доступа.

2. Требования к работам по технической защите информации в АС от ее утечки по техническим каналам.

В данной статье наиболее подробно рассмотрен вопрос защиты информации в АС от несанкционированного доступа.

Понятие конфиденциальной информации

В соответствии с нормативным документом, известным как СТР-К, «конфиденциальная информация» — информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Если с первой частью определения «конфиденциальной информации» все понятно, то во второй части возникает вопрос: «к какой информации в соответствии с законодательством ограничивается доступ?».

Ответ на данный вопрос можно получить в Указе Президента Российской Федерации от 6 марта 1997 г. № 188, которым утвержден перечень сведений конфиденциального характера.

К конфиденциальной информации относятся не только «тайна следствия и судопроизводства», «служебная тайна», но и «коммерческая тайна» и актуальные на сегодняшний день «персональные данные».

В каждой организации для автоматизации повседневной деятельности, в том числе и кадровой работы, применяются средства вычислительной техники (СВТ). Однако только немногие понимают, что для электронной обработки сведений (или баз данных) о сотрудниках организации необходимо предварительно провести комплекс мероприятий по защите информации, обрабатываемой СВТ.

Проверка соответствия защиты конфиденциальной информации от НСД требованиям руководящих документов

При оценке эффективности организации работ по защите информации в автоматизированных системах от несанкционированного доступа и их соответствия нормативно-методическим документам необходимо обращать внимание на следующие требования:

1). Документальное оформление перечня сведений конфиденциального характера, в том числе с учетом ведомственной и отраслевой специфики этих сведений.

Первоочередным мероприятием при создании системы защиты конфиденциальной информации в организации является разработка «Перечня информации конфиденциального характера». При этом необходимо отметить то, что при получении «Перечня...» из вышестоящей организации (структуры) необходимо провести его доработку (уточнение) по специфике работы самой организации.

2). Правильность проведения классификации автоматизированных систем и наличие актов классификации.

При проверке правильности проведения классификации рассматривается ряд внутренних документов проверяемой организации, таких как:

«Перечень защищаемых информационных ресурсов автоматизированной системы и их уровень конфиденциальности»;

«Перечень лиц, имеющих доступ к штатным средствам автоматизированной системы, с указанием их уровня полномочий»;

«Матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам автоматизированной системы»;

«Режим обработки данных в автоматизированной системе».

Итоговым документом при проведении классификации является «Акт классификации...», форма которого приведена в одном из приложений СТР-К.

3). Учет и надежное хранение бумажных и машинных носителей конфиденциальной информации и их обращение, исключающее хищение, подмену и уничтожение.

Как правило, проверка учета включает следующие вопросы:

наличие регламентирующих документов по учету носителей конфиденциальной информации (приказы, распоряжения, инструкции);

наличие журналов (книг) учета (выдачи, размножения и т. д.).

4). Резервирование технических средств, дублирование массивов и носителей информации.

Как один из способов защиты информационных ресурсов от искажения и уничтожения в организациях проводится резервирование технических средств, дублирование массивов и носителей информации.

Необходимо помнить, что отсутствие резервирования информации различного характера может привести к «плачевным» последствиям. Примеров этому — множество. Приведу один из них. В ходе одной из командировок ответственный за информационную безопасность организации поделился фактом

из жизни. В 2003 г. у них в организации был сильный пожар. Сгорели все компьютеры, в том числе с носителями информации. При этом резервированию должного внимания никто не уделял. На удивление руководства организации, большинство сотрудников самопроизвольно проводили резервирование информации на собственные носители. Благодаря этому информацию смогли восстановить в течение недели. Но могло быть и хуже.

5). Использование сертифицированных технических средств обработки, передачи и хранения информации.

Для повышения уровня защищенности информации рекомендуется использовать сертифицированные по требованиям безопасности информации средства вычислительной техники. Как правило, в организациях приобретаются средства вычислительной техники той конфигурации, которая прошла сертификацию на соответствие требованиям ГОСТов. Однако сертификаты при покупке зачастую просто остаются в магазинах. Обращаю внимание, что «ТСО'95», «ТСО'03» и т. д. являются международными стандартами и наличие наклеек на средствах вычислительной техники не говорит об их соответствии российским стандартам. Поэтому при проверке должны проверяться сертификаты или их копии на соответствие российским стандартам.

6). Использование сертифицированных средств защиты информации и их соответствие классу защищенности.

По данному вопросу существует множество споров и разногласий. Основной причиной тому являются разногласия в требованиях некоторых документов по защите конфиденциальной информации. Так, в СТР-К указано, что защита конфиденциальной информации должна осуществляться *сертифицированными* по требованиям безопасности информации средствами защиты. Порядок сертификации определяется законодательством Российской Федерации. Однако при отнесении автоматизированной системы к 3Б, 2Б, 1Г, 1Д классам защищенности от несанкционированного доступа руководящим документом Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» использование *сертифицированных* средств защиты *не предусмотрено*.

При проверке данного вопроса необходимо учесть, что «Сборник руководящих документов по защите информации от несанкционированного доступа» был разработан в 1998 г., когда не учитывались новые информационные технологии, а СТР-К — в 2002 г., когда появились наиболее современные операционные системы, новое коммутационное оборудование, новые стандарты.

7). Предотвращение внедрения в автоматизированные системы программ-вирусов, программных закладок.

Применение антивирусных программ и поиск программ-шпионов считается не роскошью, а скорее необходимостью. Теперь практически каждый вирус содержит в себе модули для кражи информации.

В большинстве проверенных организаций применяются антивирусные программы нелицензионного производства. В то же время необходимо понимать, что нелицензионное программное обеспечение может быть источником вирусов. Поэтому для защиты информации от программно-математических воздействий (вирусы, «черви», «троянские кони») необходимо применять лицензионные антивирусные программы. При этом документально назначить ответственных за антивирусную безопасность и регламентировать периодичность обновления антивирусных баз.

8). Организация работы при подключении локальной вычислительной сети к другой автоматизированной системе.

Данный вопрос целесообразнее подразделить на два подпункта:

- подключение локальной вычислительной сети к другим автоматизированным системам без выхода в сети общего пользования;
- подключение к сетям общего пользования.

При проверке организации работ по подключению автоматизированных систем к другим информационным системам без выхода в сети общего пользования особое внимание необходимо обратить на наличие и правильность установки сертифицированных по требованиям безопасности средств защиты и используемых каналов передачи данных.

Так, в соответствии с СТР-К для организации взаимодействия локальных вычислительных сетей с классом защищенности 1Г должен применяться сертифицированный по требованиям безопасности межсетевой экран не ниже класса 4, а для классов защищенности 1Д, 2Б и 3Б класса — 5 или выше.

Передача информации по каналам связи, выходящим за пределы контролируемой зоны, должна осуществляться по защищенным каналам связи, в том числе защищенным волоконно-оптическим линиям связи, а при использовании открытых каналов связи должны применяться сертифицированные Федеральной службой безопасности криптографические средства защиты.

В соответствии с требованиями СТР-К, при взаимодействии локальных вычислительных сетей должен осуществляться постоянный контроль сертифицированными по требованиям безопасности информации средствами контроля. Коммуникационное оборудование и все точки соединения с локальными периферийными устройствами локальных вычислительных сетей должны располагаться в пределах контролируемой зоны.

9). Наличие и содержание (качество исполнения) организационно-распорядительной и рабочей документации по эксплуатации системы защиты информации от несанкционированного доступа.

В документах должны отражаться следующие вопросы:

- реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к информации и связанным с ее использованием работам, документам;
- ограничение доступа персонала и посторонних лиц в помещения, где размещены средства информатизации и коммуникационное оборудование, а также хранятся носители информации;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей автоматизированных систем и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц.

Итогом изучения организационно-распорядительной документации должна быть проверка выполнения их требований, а также:

проверка размещения объектов вычислительной техники, обрабатывающих конфиденциальную информацию, на максимально возможном расстоянии от границ контролируемой зоны;

проверка правильности размещения дисплеев и других средств отображения информации, исключающего ее несанкционированный просмотр;

организация физической защиты помещений и собственно технических средств обработки информации с использованием технических средств охраны, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение документов и носителей информации, самих средств информатизации.

Проверка защиты конфиденциальной информации от ее утечки по техническим каналам.

При проверке защищенности СВТ, обрабатывающей конфиденциальную информацию, от утечки по техническим каналам необходимо обратить внимание на следующие вопросы:

размещение понижающих трансформаторных подстанций электропитания и контуров заземления объектов защиты;

использование сертифицированных систем гарантированного электропитания (источников бесперебойного питания);

развязка цепей электропитания объектов защиты с помощью сетевых помехоподавляющих фильтров, блокирующих (подавляющих) информативный сигнал;

электромагнитная развязка между информационными цепями, по которым циркулирует защищаемая информация, и линиями связи.

Завершающим этапом всех мероприятий по защите конфиденциальной информации является проведение аттестации объектов информатизации. По окончании аттестации выдается «Аттестат соответствия...», подтверждающий отсутствие технических каналов утечки, а главное — правильность выполненного вами комплекса мероприятий.

В завершение своей статьи хотелось бы сказать словами народной мудрости: «Скупой платит дважды», т. е. сэкономили на одном из мероприятий по защите информации — увеличили шансы ее утечки, что зачастую используется нарушителями и приводит к различным негативным последствиям.

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Об утверждении положения о Федеральной службе по техническому и экспортному контролю».
2. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня конфиденциальной информации».
3. Указ Президента Российской Федерации от 19 мая 2004 г. № 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена» (в редакции Указов Президента РФ от 22 марта 2005 г. № 329, от 3 марта 2006 г. № 175).
4. Сборник руководящих документов по защите информации от несанкционированного доступа, 1998 г.
5. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам, 2002 г.