В. ЛИМ, Ю. АРБУЗОВ, В. ХИМИЧ, С. ДЗИОЕВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМАХ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ СТРОИТЕЛЬНОГО ПРОИЗВОДСТВА ПРИ КАПИТАЛЬНОМ РЕМОНТЕ МАГИСТРАЛЬНЫХ ГАЗОПРОВОДОВ

Задачи обеспечения информационной безопасности (ИБ) являются в настоящее время очень актуальными для предприятий топливно-энергетического комплекса (ТЭК) вследствие повсеместного внедрения информационных технологий в их производственно-хозяйственную деятельность. Информационная безопасность, наряду с промышленной, экологической, экономической, физической и другими видами безопасности, вследствие влияния объективных факторов становится неотъемлемой составной частью общей системы безопасности любого предприятия ТЭК. Широкое внедрение в инфраструктуру предприятий современных телекоммуникационных систем, в том числе с выходом в интернет, средств электронно-вычислительной техники, специальных и других технических средств, как правило, иностранного производства, объективно ведет к увеличению вероятности утечки конфиденциальной информации. Нарушения системы информационной безопасности могут привести к очень серьезным экономическим потерям, создать угрозу жизни и здоровью персонала предприятий и населения. Очевидно, что для обеспечения допустимого уровня риска ИБ требуется применение научно обоснованных подходов, базирующихся на современной нормативной базе и практическом опыте отечественных и зарубежных предприятий.

Система обеспечения информационной безопасности любого предприятия будет эффективной, только являясь составным элементом комплексной интегрированной системы безопасности предприятия (КИСБ) [1]. Под КИСБ опасных производственных объектов понимается совокупность информационных, технических и организационных мероприятий, позволяющая осуществить автоматизированное формирование (получение), доставку, обработку, анализ и формализованное представление информации по признакам наступления на контролируемых объектах опасных ситуаций с целью принятия своевременных мер по их предупреждению и пресечению. Очевидно, что КИСБ должна обеспечивать процессы или действия, имеющие своим результатом как целостность информационно-технических систем предприятия, так и всей его инфраструктуры в целом. Именно комплексный подход к обеспечению ИБ позволит использовать для этих целей уже имеющиеся на предприятии системы физической безопасности (систему охранной сигнализации, систему контроля и управления доступом, систему охраны локальных зон, средства антитеррористической защиты), системы экономического учета, системы промышленной, энергетической и экологической безопасности.

Обеспечение ИБ любого предприятия - это непрерывный процесс, объединяющий правовые, организационные и технические меры защиты. Чтобы добиться его управляемости, необходимо регулярно проводить аудит системы защиты информации, в идеале охватывая все виды угроз, а также динамику их развития. Тенденции повсеместной информатизации наиболее характерны для тех отраслей экономики, которые обладают разветвленной территориально распределенной производственной инфраструктурой. В большинстве случаев такие производства применяют потенциально опасные для окружающей среды и человека технологии.

Это прежде всего относится к предприятиям транспорта, энергетики, химической промышленности, а также добывающих отраслей, где существуют непрерывные технологические циклы. Большинство элементов такой инфраструктуры крайне чувствительно к любым деструктивным воздействиям. Кроме техногенного аспекта воздействия таких производств на окружающую среду всерьез рассматриваются проблемы, непосредственно связанные с возможным проявлением технологического терроризма. В этих условиях задача обеспечения защиты информационных ресурсов таких предприятий приобретает одно из первостепенных значений [2].

Процесс информатизации управленческих структур и предприятий ОАО «Газпром» обусловил и появление новых видов угроз информационной безопасности, которые направлены, прежде всего, на системы управления и связи, информационно-телекоммуникационные системы (ИТКС) критически важных объектов, которые наиболее подвержены деструктивным информационным воздействиям - несанкционированным информационным воздействиям на информационную систему, приводящим к выводу системы из строя или к нарушению функционирования этой системы в результате разрушения (нарушения) ее информационно-технологической структуры.

Отсутствие должного внимания к обеспечению информационной безопасности этих систем может не только привести к значительному экономическому ущербу, но и оказать негативное воздействие на экологическую обстановку в регионе и даже вызвать в ряде случаев катастрофические последствия.

Наиболее актуальными в настоящее время являются вопросы обеспечения безопасности информации в ключевых системах информационной инфраструктуры (КСИИ), к которым должны быть отнесены системы автоматизированного проектирования строительного производства (САПР СП) при капитальном ремонте магистральных газопроводов, нарушение штатного режима функционирования которых может привести к возникновению чрезвычайной ситуации.

ЛИМ Владимир Григорьевич *- кандидат технических наук, доцент Астраханского государственного университета.*
Адрес: 414000, г. Астрахань, Главпочтамт, А/Я 122
e-mail: lim@astranet.ru
АРБУЗОВ Юрий Алексеевич *- главный инженер ООО «Газпром трансгаз Нижний Новгород».*
Адрес: 603950, г. Нижний Новгород, ул. Звездинка, 11
e-mail: wit72@mail.ru
ХИМИЧ Виталий Николаевич *- главный инженер ООО «Передвижная механизированная колонна № 4».*
Адрес: 117418, г. Москва, ул. Цюрупы, 1, стр. 6
e-mail: pmk@rambler.ru
ДЗИОЕВ Сослан Казбекович *- генеральный директор ООО «Спецремдиагностика».*
Адрес: 117447, г. Москва, ул. Б. Черемушкинская, 19 «А»
e-mail: srd-info@bk.ru

При этом не обязательно, чтобы в КСИИ обрабатывалась информация ограниченного доступа. В подобных системах может циркулировать открытая информация, например, технологическая информация.

Основной защищаемой информацией в САПР СП объектами ТЭК является технологическая информация (программно-техническая, командная, измерительная), которая не относится к информации ограниченного доступа. Информация ограниченного доступа в этих системах защищается в соответствии с действующими требованиями и нормами по защите и обработке конфиденциальной информации.

В САПР СП, как и в большинстве автоматизированных систем, имеющих в своем составе несколько подсистем различного уровня доступа, задачи комплексной защиты информации реализованы только в подсистемах верхнего уровня, обрабатывающих информацию ограниченного распространения либо управляющих технологическими процессами. Это позволяет реализовать угрозу утечки охраняемых сведений путем программной логической обработки информации из открытых баз данных подсистем нижнего уровня. Это может привести не только к потере сведений ограниченного распространения, но и к выявлению уязвимых звеньев системы для последующей разработки информационных атак на нее.

В составе многоуровневых информационных систем в подсистемах верхнего уровня зачастую пренебрегают средствами антивирусной защиты, а также средствами контроля целостности системы, что мотивируется полной локальностью подсистемы и невозможностью удаленного доступа. При этом не учитывается так называемый человеческий фактор, возможность экстремистских и террористических проявлений. Имеется реальная вероятность несанкционированной установки вредоносных программ, способных воздействовать на основные программно-технические комплексы САПР СП, в том числе и автоматизированных систем управления технологическими процессами опасных производственных объектов. Нарушение штатного функционирования таких систем способно привести к серьезным экологическим и социальным катастрофам.

САПР СП создаются на базе программно-технических средств импортного производства, в их составе повсеместно используются англоязычные версии операционных систем, не прошедшие сертификацию на соответствие требованиям информационной безопасности. При проектировании системы защиты информации САПР СП также превалирует формальный подход. Формально перечень подсистем системы информационной безопасности обычно соответствует требованиям Гостехкомиссии России, но фактический состав решаемых ими задач, как правило, узок и не соответствует современным требованиям, предъявляемым к защите ИТКС. Например, в перечень инструментальных средств подсистемы обнаружения вторжений включаются только средства антивирусной защиты, а программы, реализующие функции обнаружения сетевых атак, отсутствуют. Имеют место случаи реализации системы информационной безопасности стандартными средствами операционных систем (ОС) производства Microsoft, что совершенно недостаточно для ключевых систем. Эти операционные системы содержат значительное количество документированных уязвимостей, т.к. установка пакетов обновлений ОС и приложений, как правило, не производится. Это существенно повышает риски проявления внутренних угроз ИБ. Задача потенциальных злоумышленников значительно облегчается вследствие ошибок при проектировании средств аутентификации и авторизации пользователей САПР СП, а также аудита и средств регистрации событий. Реализация таких подсистем системы ИБ, как подсистема управления доступом, подсистема регистрации и учета, подсистема обеспечения целостности, сводится к настройке и применению стандартных средств операционной системы. Широкое использование ролевой аутентификации, позволяющей любому физическому лицу из обслуживающего персонала САПР СП авторизоваться в любой роли, может привести к возможности получения контроля над системой лицом, не имеющим соответствующих полномочий. Вместе с тем, проблема контроля доступа может быть успешно решена при помощи смарт-карт.

Проектно-техническая документация по информационной безопасности САПР СП разрабатывается на основе устаревших нормативно-технических документов. При этом обычно не производится оценка рисков нарушения системы защиты информации и не выполняется оптимизация затрат на создание подсистемы ИБ.

Значительная часть автоматизированных систем введена в эксплуатацию 15-20 лет назад. Несмотря на модернизацию, в состав этих систем по-прежнему входит большое количество устаревшего оборудования, а также много устройств специального назначения с ограниченной функциональностью, находящихся в экстремальных условиях эксплуатации.

Несмотря на то, что САПР СП имеют ограниченную функциональность, обусловленную их прямым назначением, а информационные потоки между САПР СП и АСУ организационно-экономического назначения жестко регулируются, в САПР СП существуют те же угрозы информационной безопасности, что и в корпоративных сетях, а также дополнительные угрозы.

В результате реализации этих угроз возможны: выход из строя технологического оборудования, нанесение экологического ущерба окружающей среде, а также здоровью и жизни людей.

Под угрозой (в общем смысле) обычно понимают потенциально возможное событие (воздействие, процесс или явление), которое может привести к нанесению ущерба чьим-либо интересам. В дальнейшем под угрозой безопасности САПР СП будем понимать возможность воздействия на САПР СП или непосредственно на объект управления, которое прямо или косвенно может нанести ущерб безопасности САПР СП.

Существует обширный перечень угроз информационной безопасности автоматизированных систем, содержащий сотни позиций. Рассмотрение всех возможных угроз информационной безопасности выполняется с целью определения полного набора требований к проектируемой системе защиты информации (СЗИ).

Необходимость классификации угроз информационной безопасности САПР СП обусловлена тем, что хранимая и обрабатываемая информация в современных автоматизированных системах подвержена воздействию чрезвычайно большого числа факторов, в силу чего становится невозможным формализовать задачу описания полного множества угроз. Поэтому для защищаемой системы обычно определяют не полный перечень угроз, а перечень классов угроз.

Как правило, для качественного определения мер защиты необходимо знать, «от кого защищать», т.е. выявить все возможные угрозы.

Модель угроз безопасности информации в КСИИ содержит систематизированные сведения о возможных угрозах безопасности информации на типовых объектах информатизации (автоматизированных системах, созданных на базе средств вычислительной техники (СВТ), автономных или подключаемых к другим вычислительным сетям, помещениях со средствами автоматизации и связи и т. п.).

Модель угроз безопасности информации в КСИИ разрабатывалась с учетом современных тенденций разви-

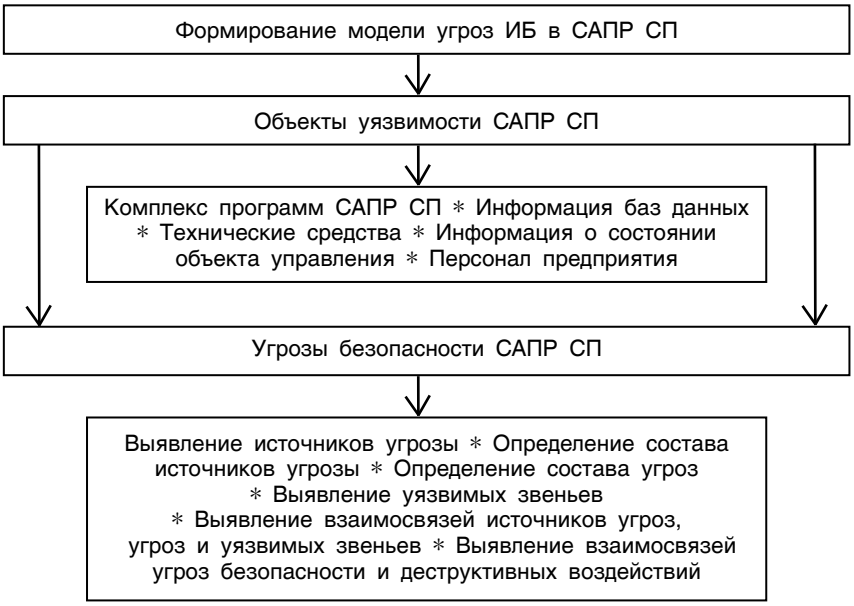

Рис. 1. *Схема алгоритма формирования модели угроз*

тия СВТ и компьютерных сетей, технологий промышленного шпионажа.

Документами вводится понятие безопасности информации (БИ) - это состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т. п.

Под угрозой безопасности информации понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными или непреднамеренными воздействиями на нее. Обобщенная схема алгоритма построения модели угроз информационной безопасности в САПР СП представлена на **рис.1**.

Последствием реализации угрозы может быть нарушение конфиденциальности, целостности или доступности информации.

Классификация возможных угроз информационной безопасности САПР СП может быть проведена по определенным базовым признакам.

1. По природе возникновения: природные (стихийные); техногенные; антропогенные.

2. По степени преднамеренности проявления: угрозы, вызванные ошибками или халатностью персонала, например, некомпетентное использование средств защиты, ввод ошибочных данных и т.п.; угрозы преднамеренного действия, например, действия злоумышленников.

3. По положению источника угроз: вне контролируемой зоны САПР СП, например, перехват данных, передаваемых по каналам связи, перехват побочных электромагнитных, акустических и других излучений устройств; в пределах контролируемой зоны САПР СП, например, применение подслушивающих устройств, хищение распечаток, записей, носителей информации и т.п.; непосредственно в САПР СП, например, некорректное использование ресурсов автоматизированной системы.

4. По источнику угрозы: внешние угрозы, источниками которых являются органы и подразделения разведок иностранных государств, криминальных структур, физические лица, не относящиеся к персоналу объекта информатизации, деятельность которых направлена на нанесение ущерба безопасности информации, а также материальные объекты или физические явления, функционирование или существование которых создает опасность для информации; внутренние угрозы, источниками которых являются субъекты в составе объекта информатизации, деятельность которого наносит или может нанести ущерб безопасности информации.

5. По степени воздействия на САПР СП: пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании САПР СП, например, угроза копирования секретных данных; активные угрозы, которые при воздействии вносят изменения в структуру и содержание САПР СП, например, внедрение «троянских коней» и вирусов.

6. По виду нарушения информационной безопасности: приводящие к нарушению доступности; приводящие к нарушению целостности; приводящие к нарушению конфиденциальности.

7. По объекту воздействия: направленные на информацию, которой оперирует персонал объекта информатизации (ОИ); направленные на информацию, обрабатываемую или хранимую техническими средствами (аппаратурой в составе ОИ); направленные на информацию, передаваемую по линиям передачи данных.

8. По характеру воздействия на защищаемую информацию: утечки информации (хищения, разглашения); утраты информации (уничтожения, потери); модификации информации (несанкционированного внесения изменений); блокирования информации.

9. По способу реализации: угрозы утечки по техническим каналам; угрозы, связанные с несанкционированным доступом (НСД) к информации, в том числе угрозы программно-математического воздействия (ПМВ) на информацию.

Существуют и другие признаки классификации угроз ИБ САПР СП [3].

Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для анализа риска реализации угроз и формулирования требований к системе защиты информации. Кроме выявления возможных угроз, целесообразно проведение анализа этих угроз на основе их классификации по ряду признаков. Каждый из признаков классификации отражает одно из обобщенных требований к системе защиты. Угрозы, соответствующие каждому признаку классификации, позволяют детализировать отражаемое этим признаком требование.

Литература:

1. Мишин Е.Т., Оленин Ю.А., Капитонов А.А. Системы безопасности предприятия - новые акценты // Конверсия в машиностроении. - 1998. - № 4.

2. Ефимов А.И. Информационная безопасность ОАО «Газпром»: проблемы гиганта. - Information Security // Информационная безопасность. - 2006. - № 5. - С. 4-6.

3. Шивдяков Л.А. Проблемы обеспечения информационной безопасности в ключевых системах информационной инфраструктуры органов государственного управления. Модель угроз безопасности информации в КСИИ // Безопасность информационных технологий. - 2009. - № 2.