УДК 621.391(075.8)

Трещев Иван Андреевич
ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет»
Россия, Комсомольск-на-Амуре
Заведующий кафедрой «Информационная безопасность автоматизированных систем»
Кандидат технических наук
E-Mail: kalkt@yandex.ru

О классификации угроз безопасности конфиденциальной информации предприятия

Аннотация. В данной работе рассмотрен вопрос классификации угроз безопасности конфиденциальной информации предприятия на основе источников угроз. Выделены основные источники угроз. Проанализированы способы реализации соответствующих угроз.

Ключевые слова: информационная безопасность, система защиты информации, угрозы безопасности.

Введение

При разработке, построении и внедрении комплексной системы защиты конфиденциальной информации необходимо придерживаться определенной методики проведения исследований, проектирования, формирования системы и ее эксплуатации. Учитывая сложность системы защиты конфиденциальной информации необходимо использовать разные принципы для ее построения, акцентируя внимание на специфику решаемой задачи.

Система защиты должна быть спроектирована таким образом, чтобы обеспечить защищенность информации от атак потенциальных нарушителей и выполнения требований законодательства РФ по защите конфиденциальной информации и требований нормативно-методических документов органов, регулирующих защиту информации ограниченного распространения. Контроль и надзор за выполнением требований федерального законодательства о защите конфиденциальной информации, в соответствии с п. 3 ст. 19 Федерального закона «О персональных данных», осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с конфиденциальной информацией, обрабатываемыми в информационных системах.

Федеральными органами, регулирующими деятельность в сфере обработки персональных данных (регуляторами), являются:

- Роскомнадзор (Федеральная служба по надзору в сфере связи и массовых коммуникаций) - осуществляет контроль и надзор за соответствием обработки конфиденциальной информации требованиям законодательства;
- ФСТЭК России (Федеральная служба по техническому и экспортному контролю) - осуществляет контроль и надзор за методами и способами защиты информации в информационных системах с использованием технических средств[2];
- ФСБ России (Федеральная служба безопасности РФ) - осуществляет контроль и надзор за методами и способами защиты информации в информационных системах с использованием криптографических средств защиты информации [1].

Под угрозами безопасности информационной системы понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации или несанкционированными, непреднамеренными воздействиями на нее[3]. Таким образом, угрозы безопасности информации могут быть связаны как с непреднамеренными действиями персонала информационной системы, так и со специально осуществляемыми неправомерными действиями отдельных организаций и граждан, а также иными источниками угроз.

Зарубежный и отечественный опыт в области защиты конфиденциальной информации показывает, что эффективной может быть только комплексная защита, сочетающая в себе такие направления защиты как правовая, организационная и инженерно-техническая.

Комплексный характер защиты информации проистекает из комплексных действий злоумышленника, стремящихся добыть важную для себя информацию любыми методами и средствами. В связи с этим угрозы безопасности конфиденциальной информации предприятия следует классифицировать на основе источника.

Классификация источников угроз

Все источники угроз безопасности информации можно разделить на три основные группы:

- обусловленные действиями субъекта (антропогенные источники угроз);
- обусловленные техническими средствами (техногенные источники угрозы);
- обусловленные стихийными источниками.

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Антропогенные источники угроз по отношению к информационной системе могут быть как внешними, так и внутренними.

Среди внешних антропогенных источников можно выделить случайные и преднамеренные источники.

Случайные (непреднамеренные) источники могут использовать такие уязвимости, как ошибки, совершенные при проектировании информационной системы предприятия и ее элементов, ошибки в программном обеспечении; различного рода сбои и отказы, повреждения, проявляемые в информационной системе. К таким источникам можно отнести персонал поставщиков различного рода услуг, персонал надзорных организаций и аварийных служб и т.п. Действия (угрозы), исходящие от данных источников, совершаются по незнанию, невнимательности или халатности, из любопытства, но без злого умысла

Преднамеренные источники проявляются в корыстных устремлениях нарушителей[4]. Основная цель таких источников – умышленная дезорганизация работы, вывод систем предприятия из строя, искажение информации за счет проникновения в информационные ресурсы предприятия путем несанкционированного доступа.

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся:

- основной персонал (пользователи, программисты, разработчики);
- представители службы защиты информации;
- вспомогательный персонал (уборщики, охрана);
- технический персонал (жизнеобеспечение, эксплуатация).

Для внутренних источников угроз особое место занимают угрозы в виде ошибочных действия и (или) нарушений требований эксплуатационной и иной документации сотрудниками учреждения.

Необходимо учитывать также, что особую группу внутренних антропогенных источников составляют лица с нарушенной психикой, которые могут быть из числа основного, вспомогательного и технического персонала, а также представителей службы защиты информации. Данная группа рассматривается в составе перечисленных выше источников угроз, но методы парирования угрозам для этой группы могут иметь свои отличия.

Наибольшую опасность представляют преднамеренные угрозы, исходящие как от внешних, так и от внутренних антропогенных источников.

Необходимо рассматривать следующие классы таких угроз:

- угрозы, связанные с преднамеренными действиями лиц, имеющими доступ к информационным системам предприятия, включая пользователей и иных сотрудников предприятия, реализующими угрозы непосредственно внутри предприятия (внутренний нарушитель);
- угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к информационным системам предприятия и реализующими угрозы из внешних сетей связи общего пользования или сетей международного информационного обмена;
- угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к информационным системам и реализующими угрозы по техническим каналам утечки информации.

Техногенные источники угроз напрямую зависят от свойств техники. Данные источники также могут быть как внешними, так и внутренними.

К внешним источникам относятся инфраструктурные элементы информационных систем: средства связи (телефонные линии, линии передачи данных и т.п.), сети инженерных коммуникаций (водоснабжение, канализация, отопление и пр.).

К внутренним источникам относятся некачественные технические и программные средства обработки информации, вспомогательные средства (охраны, сигнализации, телефонии), другие технические средства, применяемые в информационных системах, а также вредоносное программное обеспечение и аппаратные закладки.

Стихийные источники угроз отличается большим разнообразием и непредсказуемостью[1] и являются, как правило, внешними по отношению к предприятию. Под ними, прежде всего, рассматриваются различные природные катаклизмы: пожары, землетрясения, ураганы, наводнения. Возникновение этих источников трудно спрогнозировать и им тяжело противодействовать, но при наступлении подобных событий нарушается штатное функционирование самой инфраструктуры предприятия и ее средств защиты, что потенциально может привести к нарушению конфиденциальности, целостности, доступности и других характеристик безопасности информации.

Как правило, защита от угроз, исходящих от техногенных и стихийных источников угроз безопасности информации, в основном регламентируется инструкциями, разработанными и утвержденными оператором с учетом особенностей эксплуатации информационных систем предприятия и действующей нормативной базой учреждения

ЛИТЕРАТУРА

1. Романец, Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.
2. Галатенко, В.А. Основы информационной безопасности: курс лекций: учеб. пособие / В.А. Галатенко. – 3-е изд. – М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2006. – 208 с.
3. Малюк, А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин. – М.: Горячая линия-Телеком, 2001. – 148 с.
4. Норткат, С. Обнаружение нарушений безопасности в сетях, 3-е издание / С. Норткат, Д. Новак; пер. с англ. В.С. Иващенко. – М.: Вильямс, 2003. – 448 с.

Ivan Treschev
Komsomolsk-on-Amur state technical University
Russia, Komsomolsk-on-Amur
E-Mail: kalkt@yandex.ru

On the classification of threats to the security of confidential company information

Abstract. In this paper we consider the question of the classification of threats to the security of confidential information on a source-based threats. The basic sources of threats. Analyzed by means of the implementation of relevant threats.

Keywords: information security, security system, security threats.

REFERENCES

1. Romanec, Ju.V. Zashhita informacii v komp'juternyh sistemah i setjah / Ju.V. Romanec, P.A. Timofeev, V.F. Shan'gin. – 2-e izd., pererab. i dop. – M.: Radio i svjaz', 2001. – 376 s.
2. Galatenko, V.A. Osnovy informacionnoj bezopasnosti: kurs lekcij: ucheb. posobie / V.A. Galatenko. – 3-e izd. – M.: INTUIT.RU «Internet-universitet Informacionnyh Tehnologij», 2006. – 208 s.
3. Maljuk, A.A. Vvedenie v zashhitu informacii v avtomatizirovannyh sistemah / A.A. Maljuk, S.V. Pazizin, N.S. Pogozhin. – M.: Gorjachaja linija-Telekom, 2001. – 148 s.
4. Nortkat, S. Obnaruzhenie narushenij bezopasnosti v setjah, 3-e izdanie / S. Nortkat, D. Novak; per. s angl. V.S. Ivashhenko. – M.: Vil'jams, 2003. – 448 s.