Кулькина Нина Владимировна
студентка
Михнев Илья Павлович
канд. техн. наук, доцент, доцент,
Заслуженный работник науки и образования
Волгоградский институт управления (филиал)
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте РФ»
г. Волгоград, Волгоградская область

ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И КОНТРОЛЬ ДЕЯТЕЛЬНОСТИ ПЕРСОНАЛА НА ПРЕДПРИЯТИЯХ

Аннотация*: в статье рассмотрены основные понятия защиты конфиденциальной информации. Охарактеризованы организационные и технические средства защиты информации. Проанализированы основные направления организационных мероприятий и особенности контроля деятельности персонала на предприятиях.*

Ключевые слова*: конфиденциальная информация, средства защиты информации, информационная безопасность, контроль деятельности персонала, компьютерные преступления, криптографическая защита.*

В условиях развития рыночной экономики информация становится самым ценным товаром, поэтому главной задачей для субъектов хозяйственной деятельности является защита конфиденциальной информации, что позволяет обеспечить компании экономическую безопасность, избежать банкротства, защитить себя от недобросовестной конкуренции и коммерческого шпионажа, предупредить рейдерские атаки. Важнейшей характеристикой информации считается ее ценность (полезность), которая, как правило, определяется ее владельцем. Именно вследствие утечки коммерческой информации национальные компании очень часто страдают от снижения возможности продажи лицензий на собственные научные разработки, от потери приоритета в освоенных областях научно-

технического прогресса, от роста затрат на переориентацию деятельности исследовательских подразделений, от роста затрат предприятия на создание новой рыночной стратегии и многих других.

Одним из видов противоправных посягательств на экономическую безопасность предприятия являются компьютерные преступления. Непосредственным объектом компьютерных преступлений является как информация, так и сами компьютерные программы. Посягательство на информацию, которая охраняется, могут быть различными: кража носителя информации, нарушение средств защиты информации, использование чужого имени, изменение кода или адреса технического устройства, предоставления фиктивных документов на право доступа к информации, установка аппаратуры, что ведет несанкционированную запись. Последствия противоправных посягательств на конфиденциальную информацию предприятия могут привести к изменению содержания информации по сравнению с той, что была раньше, блокированию информации, уничтожению информации без возможности ее восстановления, нарушению работы компьютеров и компьютерных сетей [1].

Зарубежные специалисты разработали различные классификации способов совершения компьютерных преступлений. Так, кодификатор Генерального Секретариата Интерпола содержит специальные коды, характеризующие компьютерные преступления, они имеют идентификатор, начинающийся с буквы Q. Для характеристики преступления могут использоваться до пяти кодов, которые располагаются в порядке уменьшения значимости преступления. Так, несанкционированный доступ и перехват информации (QA) включает в себя следующие виды компьютерных преступлений [2]:

– «компьютерный абордаж» – доступ к компьютеру или к сети без права на это. Этот вид преступления используется для проникновения в чужие информационные сети;

– перехват – перехват информации с помощью технических средств, без права на это. Он осуществляется или путем подключения внешних коммуникационных каналов, или путем подключения к периферийным устройствам.

Еще одним видом компьютерных преступлений является внесение изменений в компьютерных данных QDL/QDT:

– логическая бомба – заключается в тайном встраивании в программу набора команд, который должен сработать лишь однажды, но при определенных условиях;

– троянский конь – это тайное введение в чужую программу таких команд, которые позволяют осуществлять другие функции, не планировавшиеся владельцем программы, но одновременно сохранять и прежнюю работоспособность.

Большую опасность представляют компьютерные вирусы (QDV). Компьютерный вирус – это специальная программа, которая позволяет приписать себя к другим программам, размножается и рождает новые вирусы для выполнения различных нежелательных действий на компьютере. Понятно, что избавиться от компьютерного вируса гораздо сложнее, чем обеспечить действительные меры по его профилактике [3].

Обеспечение безопасности предпринимательской деятельности со стороны компьютерных систем представляет один из блоков проблемы защиты конфиденциальной информации. Защита должна начинаться с разработки концепции информационной безопасности компании. Механизм защиты конфиденциальной информации предусматривает как организационные, так и технические средства. Организационные средства защиты направлены на ограничение возможного несанкционированного физического доступа к документам, содержащим конфиденциальную информацию, в том числе к компьютерным сетям. Технические средства предполагают использование средств программно-технического характера, прежде всего, на ограничение доступа сотрудников компании, особенно тех, что работают с компьютерными системами, к информации, обращаться к которой они не имеют права [4]. Специалисты предлагают следующие направления технической защиты: использование средств контроля за включением питания и загрузки программного обеспечения; установка паролей; шифрование и специальные протоколы связи; дополнительная проверка аппаратуры; «цифровая подпись» и другие.

Необходимо отметить, что к числу особо сложных компонентов ИС любой природы относятся люди (сотрудники, продавцы, партнеры, клиенты, и т. д.), являющиеся главными источниками информации. Поэтому работа с кадрами – важнейшее направление деятельности по обеспечению сохранности конфиденциальной информации и защиты ее от несанкционированного доступа. Необходимо изучать весь состав работающих на предприятии специалистов, выделяя при этом тех, кто имеет доступ к особо ценной и важной информации. Особые категории работников – это кандидаты на вакантные должности и на увольнение. Эти люди, в большей мере, чем остальные, склонны к противоправным действиям, особенно последние. Объектом повышенной заботы должен быть персонал, осуществляющий сбыт продукции и обслуживающий запросы клиентов о возможностях улучшенных или новых моделей, планируемых к реализации. Сообщая дополнительную информацию о разрабатываемых изделиях, такие специалисты могут разгласить сведения, составляющие производственную или коммерческую тайну [5].

Основными принципами обеспечения информационной безопасности являются взаимная ответственность руководства и персонала предприятия, законность, достаточность, взаимодействие с государственными и частными правоохранительными органами, соблюдение оптимального баланса интересов предприятия и личности [3]. Одним из основных факторов, существенно влияющими на эффективность системы защиты конфиденциальной информации, является совокупность сил и средств предприятия, которые используются для организации защиты информации и прямо участвующих в этом процессе. Силы, а также средства разных предприятий отличают по структуре, характеру и порядку использования. Предприятия, которые осуществляют работу с конфиденциальной информацией и решают задачи по её защите на постоянной основе, а именно в каждодневной деятельности, вынуждены с данной целью основывать самостоятельные структурные подразделения и применять высокоэффективные средства защиты информации [2].

К организационным мероприятиям следует отнести:

– специальные действия, выполняемые при проектировании, строительстве и обустройстве производственных зданий и помещений;

– подбор персонала, обучение его основам, правилам и методам работы с конфиденциальной информацией, ознакомление с ответственностью, предусмотренной за нарушение правил и требований защиты информации;

– организация, поддержание и совершенствование надежного контроля за действиями посетителей и пропускного режима;

– организация надежной охраны территорий и помещений; организация использования носителей и документов конфиденциальной информации и их хранения, включая порядок учета, выдачи, исполнения и возвращения;

– назначение ответственного за защиту информации, проведение систематического контроля за персоналом, работающим с конфиденциальной информаций и т. д.

Одним из основных направлений организационных мероприятий является четкая организация системы делопроизводства и документооборота. Основным организационным мероприятием является разработка перечня охраняемых сведений и проведения аттестации помещений на предмет выработки конкретных мер по защите и обеспечению безопасности конфиденциальной информации. Важным мероприятием представляется создание на предприятии собственной службы безопасности – системы штатных органов управления и организационных формирований, предназначенных для обеспечения безопасности и защиты конфиденциальной информации [4].

Службой информационной безопасности выступает орган управления системы защиты информации. От качества создания службы информационной безопасности, а также профессиональной подготовленности её сотрудников, присутствия у них современных средств управления безопасностью особенно зависит эффективность мероприятий защиты информации. Основная цель функционирования службы информационной безопасности – с помощью организационных мер и программно-аппаратных средств избежать либо свести к минимуму

вероятность нарушения политики безопасности, или же, в крайнем случае, своевременно заметить, а также устранить последствия нарушения.

Эффективность обеспечения экономической и, в частности, информационной безопасности предприятия может быть наивысшей, если работа в службе безопасности будет престижной и высокооплачиваемой. Инженерно-техническая и технологическая защита – это совокупность технических средств и специальных органов, а также организационных мероприятий по их комплексному использованию в интересах обеспечения безопасности предприятия. По функциональному назначению инженерно-техническая и технологическая защита использует следующие средства:

- физические, которые включают различные инженерные сооружения и средства, препятствующие проникновению злоумышленников на защищаемые объекты и осуществляющие защиту информации, материальных средств, персонала, и финансов от противоправных действий;

– аппаратные, в число которых входят приборы и устройства, а также разнообразные технические решения, начиная от телефонного аппарата и кончая самыми современными автоматизированными ИС;

– программные, представляющие собой специальные программные комплексы, отдельные программы и системы разноплановой защиты информации;

– криптографические – специальные алгоритмические и математические средства, основанные на применении методов шифрования. Шифрование является механизмом эффективной логической безопасности. Оно может использоваться в интересах обеспечения и целостности, и конфиденциальности как хранимой, так и передаваемой информации. Самой определяющей частью системы шифрования является генерация и передача ключей [5].

Физическая безопасность не сводится к безопасности только вычислительного центра, тем более что ИС все более и более рассредоточиваются. Необходимо рассматривать взаимосвязь безопасности комплекса знаний, сооружений и оборудования. Безопасность ИС оценивается на основе использования таких мер, как идентификация, подтверждение подлинности, контроль доступа,

информационные права, аудит, безаварийность и конфиденциальность. Особо следует рассмотреть систему разграничения доступа к конфиденциальной информации. Защита информации в линиях связи сводится к защите содержания сообщения и защите процесса передачи данных. Исследование и анализ различных сторон практической деятельности ведущих западных и российских фирм, специальных государственных и частных служб и других организаторов и исполнителей функций обеспечения безопасности ИС показывает, что системный подход к решению проблемы защиты информации не только полезен в реальной практической деятельности, но является единственным правильным направлением достижения надежной информационной защиты.

Список литературы

1. Степанов Е.А. Информационная безопасность и защита информации: Учебное пособие / Е.А. Степанов, И.К. Корнеев. – М.: Инфра-М, 2014. – 304 с.

2. Михнев И.П. Информационная безопасность спектрометрических систем при определении радиационных характеристик в помещениях Волгоградской области / И.П. Михнев, Н.А. Сальникова // Известия Волгоградского государственного технического университета. – 2015. – №13 (177). – С. 109–113.

3. Галицкий А.В. Защита информации в сети – анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин. – М.: ДМК Пресс, 2016.

4. Михнев И.П. Информационная безопасность в современном экономическом образовании // Международный журнал прикладных и фундаментальных исследований. – 2013. – №4. – С. 111–113.

5. Михнев И.П. Информационная безопасность на просторах мобильного интернета // Образовательные ресурсы и технологии. – 2015. – №4 (12). – С. 66–70.

6. Хрусталев Е.Ю. Концептуальные основы построения системы информационной безопасности производственного предприятия [Электронный ресурс]. – Режим доступа: https://otherreferats.allbest.ru/programming/00812157_0.html (дата обращения: 04.05.2018).