АНАЛИЗ ВОЗМОЖНЫХ МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ МАЛЫХ ПРЕДПРИЯТИЙ

ANALYSIS OF POSSIBLE METHODS OF ENSURING INFORMATION SECURITY FOR SMALL ENTERPRISES

Yu. Golodkov
A. Golodkova

Summary. The article considers the issues of ensuring information security of small businesses. Attention of heads of small enterprises to the possibility of creating an information security system using inexpensive organizational legal measures.

Keywords: information security, information security, unauthorized access.

Голодков Юрий Эдуардович
ФГКОУ ВО Восточно-Сибирский институт МВД России (г. Иркутск)
Yrg27@mail.ru
Голодкова Александра Валерьевна
ФГБОУ ВО Иркутский национальный исследовательский технический университет
Alex17–27@mail.ru

Аннотация. В статье рассматриваются вопросы обеспечения информационной безопасности предприятий малого бизнеса. Обращено внимание руководителей малых предприятий на возможность создания системы защиты информации с использованием недорогих организационных правовых мер.

Ключевые слова: информационная безопасность, защита информации, несанкционированный доступ.

Для эффективного развития малых предприятий актуальным является надежная защита информации, определяющая профессиональные интересы организации. Руководители малых и, особенно, начинающих предприятий не считают первостепенной задачей обеспечение информационной безопасности деятельности всей фирмы и действий отдельных сотрудников. Отсутствие стратегии развития системы информационной безопасности предприятия приводит к повышению риска утечки информации и как следствие снижению экономических показателей. Немаловажной причиной является отсутствие квалифицированного персонала, в редких случаях небольшие компании могут похвастаться наличием в штате IT-специалиста. Обычно его функции выполняет опытный пользователь из числа штатных сотрудников или, в лучшем случае, приходящий системный администратор [1].

В данной статье не ставится задача описания современной системы обеспечения информационной безопасности, а уделяется внимание простым элементарным, но достаточно действенным мерам выявления каналов утечки информации. Для определения мероприятий по защите информации необходимо рассмотреть такие категории как требования к защищенности информации, средства защиты информации и пути повышения защищенности используемой информации.

Информационные компьютерные сети достаточно уязвима и в случае их блокирования работа всего предприятия или отдельного офиса парализуется. При работе с компьютерной информацией сотрудники организации, как правило, не подозревают о возможном копировании, модифицировании или даже потери информации. Наиболее сложными видами обнаружения информационного мошенничества являются не кража информации, а ее наблюдение, копирование и искажение. При этом страдает достоверность, точность информации, корректность принимаемых управленческих решений. Криминальные элементы могут использовать компьютерные сети и информационные технологии в преступных целях, для скрытого получения информации, подготовки и осуществления неправомерных действий в отношении коммерческих интересов.

Авторами [2] отмечается, что при решении вопросов по обеспечению безопасности используемых автоматизированных информационных систем первостепенной задачей является определение требований к уровню защиты информации, использующейся в информационной системе, который является критичным по требованию субъекта информации. Сложность задачи по обеспечению информационной безопасности определяется характером интересов субъектов информационных отношений.

В соответствии с требованиями руководящего документа [3] средства вычислительной техники (СВТ) от несанкционированного доступа подразделяются на семь классов защищенности. Первый класс отвечает самым высоким требованиям защищенности систем, седьмой класс имеет наиболее низкие показатели защищенности. Наиболее важными требованиями к защищенности СВТ являются следующие:

- надежное восстановление;
- контроль модификации;

- очистка памяти;
- идентификация и аутентификация;
- защита ввода и вывода на произвольный носитель информации и т.д.

Не обращать внимание на необходимость обеспечения информационной безопасности используемых средств вычислительной техники в информационной системе малого предприятия, ссылаясь только на вероятность отсутствия экономического интереса со стороны злоумышленников и на малый оборот денежных средств, большая стратегическая ошибка руководителя.

Руководящим документом [4] выделяется девять классов защищенности автоматизированных систем от несанкционированного доступа к информации. Для каждого класса разработаны определенные требования к средствам защиты. Классы подразделяются на три группы, состав которых определяется на основании следующих признаков:

- уровень полномочий пользователей информационной системы на доступ к конфиденциальной информации;
- наличие в информационной системе информации различного уровня конфиденциальности;
- режим обработки данных в информационной системе (коллективный или индивидуальный).

Каждая группа имеет свою иерархию классов.

Третья группа — определяет работу одного пользователя, допущенного ко всем данным автоматизированной системы, размещенной на носителях одного уровня конфиденциальности. Группа имеет два класса — 3Б и 3А.

Вторая группа — определяет работу пользователей, которые имеют одинаковые права доступа ко всем данным автоматизированной системы, хранимой и (или) обрабатываемой на носителях разного уровня конфиденциальности. Группа имеет два класса — 2Б и 2А.

Первая группа — определяет многопользовательские автоматизированной системы, где одновременно хранится и (или) обрабатываются данные разных уровней конфиденциальности, и не все пользователи имеют доступ к ней. Группа имеет пять классов — 1Д, 1Г, 1В, 1Б, 1А.

Наиболее высокие требования относятся к классу 1А.

Для каждого класса существует минимальный набор требований по защите информационной системы, среди которых можно отметить наиболее актуальные показатели защиты:

- обеспечение целостности программных средств и обрабатываемой информации;
- использование сертифицированных средств защиты;
- учет носителей информации;
- сигнализация попыток нарушения защиты;
- проверка подлинности и контроль доступа субъектов к терминалам; компьютерам, узлам сети, внешним устройствам и программам;
- шифрование конфиденциальной информации;
- физическая охрана СВТ и носителей информации и т.д.

Рассмотренная классификация может быть применена к организации системы защиты информационной системы как крупного, так и малого бизнеса, использующих конфиденциальную информацию.

Наиболее известными средствами защиты информации являются физические, аппаратные, программные и организационные.

Назначение физических и аппаратных средств защиты информации заключается в построении конкретных технических барьеров на пути злоумышленников, в исключении возможных неумышленных (по ошибке или халатности) нарушений персонала и пользователей системы, а также устранении недостатков организационных мер.

Эти средства защиты информации обладают такими важными достоинствами как надежность функционирования, независимость от субъективных факторов, высокая устойчивость от модификаций.

Недостатками являются недостаточная гибкость, громоздкость физических средств и высокая стоимость.

Программные средства защиты информации в отличие от физических и аппаратных средств располагают такими достоинствами как универсальность, гибкость, надежность функционирования, простота реализации, широкие возможности модификации и развития.

К недостаткам следует отнести снижение функциональных возможностей информационной системы, необходимость использования запоминающих устройств информационных систем, подверженность случайным или закономерным модификациям, ориентация на вполне определенные типы ЭВМ.

Организационные средства дают хорошие результаты по защите информации только в организациях с высоким уровнем правопорядка, этики и дисциплины. При этом основное внимание уделяется правовым и организационным задачам.

Организационные средства являются эффективным дополнениям к предыдущим способам защиты информации, т.к. они обладают рядом, несомненно, положительных качеств, среди которых можно отметить такие как простота реализации, гибкость реагирования на несанкционированные действия, практически неограниченные возможности изменения и развития. К сожалению, широкий перечень достоинств организационных средств ошибочно используется определенной категорией чиновников, далеких от технических вопросов, при построении системы защиты информации.

Экономия на использовании физических, аппаратных и программных средств, ориентация только на организационные средства защиты информации приводит к снижению надежности системы защиты по причине зависимости от различных субъективных факторов, к необходимости установления дополнительных правил и ограничений, дополнительной рутинной формальной деятельности и как следствие к увеличению общей организации работ на объекте.

Организационные меры в комплексном сочетании позволяют повысить эффективность применения других мер и средств защиты в части, касающейся регламентации действий людей, и требуют поддержки надежными физическими и аппаратными средствами.

При построении системы защиты информации необходимо отказаться от позиции создания абсолютно защищенной системы, т.к. это, во-первых, на практике принципиально невозможно и, во-вторых, должно быть экономически целесообразно.

Если даже реализовать абсолютно надежную систему физических, аппаратных и программных средств, блокирующих все возможные пути и каналы, слабым звеном в системе защиты остается организационная составляющая системы защиты. К сожалению, как показывает практика работы самых защищенных систем, существует возможность несанкционированного доступа с помощью воздействия на персонал, обеспечивающего функционирование безопасности всей системы, в частности, на администратора информационной системы, ответственных лиц за информационную безопасность. Служебная ответственность и дисциплина сотрудников, наделенных правами администрирования, в сочетании с техническими средствами защиты создают основу безопасности информационной системы. Стойкость данного персонала можно повышать, используя морально-этические меры, организационные (кадровые) и законодательные мероприятия. Анализируя пути повышения уровня защищенности информации в информационной системе, необходимо понимать, что абсолютной защиты не существует и наращивание потенциала технических средств защиты информации не всегда экономически целесообразно. Наиболее слабым звеном всей системы защиты является организационная составляющая по причине присутствия человеческого фактора.

Таким образом, современные информационные технологии, в особенности эффективные приемы компьютерной обработки, хранения, передачи и поиска информации, создают благоприятные условия для широкого внедрения IT разработок в коммерческой сфере. Однако при этом следует учитывать важнейший недостаток информационных технологий, в частности, уязвимость информации, передающейся по компьютерным и телекоммуникационным сетям, и, хранящейся на компьютерных цифровых носителях информации. Нарушение конфиденциальности, достоверности и своевременности информации в деятельности малых предприятий недопустимо, поэтому вопросы обеспечения информационной безопасности приобретают особую актуальность.

ЛИТЕРАТУРА

1. Особенности обеспечения информационной безопасности малого и среднего бизнеса // Новости информационной безопасности. https://www.anti-malware.ru/Small_Business_Security.
2. Баранов С. А., Голодков Ю. Э., Демаков В. И., Кургалеева Е. Е. Основы информационной безопасности в органах внутренних дел: учебное пособие. Иркутск: ФГКОУ ВПО ВСИ МВД России, 2015.
3. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». (утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.). http://base.garant.ru/197885/
4. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.). http://base.garant.ru/197886/

© Голодков Юрий Эдуардович (Yrg27@mail.ru),
Голодкова Александра Валерьевна (Alex17–27@mail.ru).
Журнал «Современная наука: актуальные проблемы теории и практики»