

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Солдатова Светлана Сергеевна,

Зими́на Виолетта Александровна

ФГБОУ ВП «Пензенский государственный университет», г. Пенза

Аннотация: в статье рассмотрен вопрос применения современных технологий с целью обеспечения информационной безопасности предприятия, проанализированы угрозы информационной безопасности организации, рассмотрены наиболее известные программы защиты информации, приведены статистические данные материальных затрат российских компаний на покупку современных систем защиты информации.

Ключевые слова: информационная безопасность, системы защиты информации, конвенциональная информация, коммерческая тайна, финансовые потери.

Вопрос обеспечения информационной безопасности предприятия является очень актуальным на сегодняшний день. В современном мире огромное значение приобретает информация, утечка конфиденциальной информации компании может принести компании глобальные финансовых потери и в некоторых случаях даже банкротство. На практике, посягательства чаще всего приходится на документы финансового значения фирмы, ее технологические и производственные разработки, логины, пароли на компьютерах, при этом посягать на конфиденциальную информацию предприятия могут как сотрудники, так и ее конкуренты [1].

Для построения эффективной системы защиты информационной безопасности организации необходимо провести анализ угроз информационной безопасности компании, которые можно подразделить на внутренние и внешние.

Внешние угрозы возникают тогда, когда злоумышленник может использовать наиболееязвимые места в системе информационной безопасности, при этом преступник использует множество инструментов для преодоления системы защиты, взлома программного обеспечения с помощью внедрения специальных вирусов, после взлома системы защиты преступник получает доступ к информации на компьютере, может ее прочитать, скопировать уничтожить и т.д. Такие угрозы исходя в большинстве случаев от конкурентов фирмы.

Внутренние угрозы возникают изнутри самой компании, поэтому зачастую их сложно выявить и еще сложнее противодействовать данной категории угроз, так как «внутренняя утечка» информации часто сопряжена с профессиональной некомпетентностью кадров, с производственными нарушениями, с управленческими ошибками или, что наиболее часто встречается на практике, с злоупотреблением должностными полномочиями, коррупционными схемами и должностными преступлениями, совершенными из корыстных побуждений.

При анализе различных категорий рисков информационной безопасности предприятия в группе «внешние угрозы» принято выделять следующие [3]:

1. «вирусы» - это одна из самых распространенных и опасных угроз для информационной безопасности компании, вирусы могут попасть на компьютер, телефон, планшет, флешку, почту и т.д. с целью «производственного шпионажа» и несанкционированной передачи конфиденциальной информации;
2. внедрение программ-шпионов для анализа сетевого трафика и получения данных о системе и состоянии сетевых соединений;
3. использование «слабых сторон» программного обеспечения с дальнейшим его взломом с целью копирования, прочтения, использования, уничтожения какой-либо информации, хранящийся на компьютере;

4. раскрытие, перехват и хищение секретных кодов и паролей с целью дальнейшего несанкционированного их использования;
5. чтение остаточной информации в памяти компьютеров и на внешних носителях;
6. блокирование работы пользователей системы программными средствами.

Внутренние угрозы в свою очередь можно подразделить на случайные и преднамеренные, случайные угрозы не имеют цели нанесения вреда компании, такие угрозы могут исходить как от ошибок и некомпетентности самих сотрудников компании, так и могут быть связаны со слабой обеспеченностью и проработкой технических вопросов обеспечения секретности конфиденциальной информации.

Внутренние угрозы информационной безопасности организации, которые сопряжены с некомпетентностью сотрудников:

- невнимательность и халатность сотрудников. Часто персонал, который не имеет цели посягательства на какую-либо информацию, в связи со своей невнимательностью и некомпетентностью наносят достаточно большой ущерб предприятию. Некоторые работники забывают поставить необходимый пароль на компьютер, отправить конфиденциальные сведения по ошибке на чужую электронную почту и т.д.;

- использование не лицензионного, или «пиратского» программного обеспечения. Многие владельцы имеют основную цель снизить свои затраты, и следовательно устанавливают на компьютеры не лицензионные программы. Но такие программы злоумышленники взламывают более простыми методами и за меньшее количество времени.

Преднамеренные внутренние угрозы сопряжены с сотрудниками фирмы. Сотрудников, которые имеют цель посягательства на информационную безопасность компании, называют «инсайдерами», категории сотрудников, которые могут перейти в ряды инсайдеров [2]:

- сотрудники, которые обижены на компанию, такими инсайдерами могут быть уволенные сотрудники, которые считают, что их уволили несправедливо;

- «нечистые» на руку сотрудники, стремящиеся подзаработать за счёт компании-работодателя, как правило, такими инсайдерами становятся сотрудники, использующие секретные информационные ресурсы компании для собственной выгоды;

- внедрённые и завербованные инсайдеры – это самый опасный и самый трудно-идентифицируемый тип внутренних злоумышленников, как правило, являются звеном преступной цепочки или членом организованной преступной группы. Такие сотрудники имеют достаточно высокий уровень доступа к конфиденциальной информации, ущерб от их действий может стать фатальным для компании, привести к серьёзным экономическим проблемам, вплоть до банкротства.

Таким образом, владельцу предприятия необходимо внимательно выбирать сотрудников, следить за их компетентностью. Кроме такого способа защиты существуют и современные технологии, включающие в себя специализированные программы защиты информации, которые минимизируют угрозы информационной безопасности предприятия:

- 1) DLP-система – система представляет собой совокупность программных продуктов, которые обеспечивают защиты конфиденциальной информации. Сама аббревиатура DLP расшифровывается как Data Leak Prevention, то есть, предотвращение утечек данных. Данная система образует безопасный цифровой «периметр» вокруг фирмы, при этом фильтрую все исходящую и входящую информацию, контролируются все данные, которые пытались скопировать на флеш, диск, отправлять по почте, распечатать, и даже перекачать на телефон или планшет. DLP-система достаточно дорогостоящая, стоимость данной системы в России составляет в среднем около 55 000 рублей [4]

2) Аура — система защиты информации от посягательств, она производится в Санкт-Петербурге, разработана Петербургским институтом информатики и автоматизации РАН, стоимость данной системы защиты составляет около 38 000 рублей. [4] Возможности данной системы: контроль всей документации, папок, файлов; контроль печати информации; шифрование электронных носителей, жестких дисков; уничтожение не достоверных объектов; регистрация всех действий сотрудников в специальном журнале; идентификация пользователей[4]

3) SysWatch Workstation – средство защиты, относящимся к классу систем предотвращения вторжений (HIPS), данный продукт осуществляет контроль над всеми процессами. Преимуществом такой программы является то, что она не требует обновления, в первую очередь она предотвращает запуск «подозрительных» приложений, проводит скрытое наблюдение за действиями пользователей, предотвращает угрозы похищения информации. Стоимость данного средства защиты составляет в России около 42 000 рублей. [3]

Наиболее крупные компания затрачивают достаточно большое количество финансовых средств на обеспечение информационной безопасности. По статистическим данным: компании-лидеры промышленного и транспортного секторов затрачивают на обеспечение информационной безопасности, в том числе на приобретение современных систем защиты около 50 млн. рублей в год; российские СМИ тратят на обеспечение информационной безопасности в среднем от 10 до 20 млн. рублей в год [5]. Минимальное количество денежных средств на обеспечение информационной безопасности выделяют образовательные учреждения, так на покупку современных систем защиты выделяется не более 1 млн. рублей в год [5].

Объем выделенных финансовых средств на обеспечение информационной безопасности организации, прежде всего зависит от годового бюджета компании. Статистика такова, что лишь 44% российских

компаний и организаций покупают современные средства защиты информации, в остальных организациях устанавливаются простейшие антивирусные программы [5].

Проблема информационной безопасности очень актуальна для большинства российских предприятий и организаций. Необходимо подчеркнуть, что, прежде всего, руководителям организаций и собственникам бизнеса необходимо быть внимательными не только при выборе технических средства защиты конфиденциальной информации, но и более тщательно подходить к отбору сотрудников для своей компании, не представлять доступ к важной конфиденциальной информации «не проверенным» сотрудникам и партнерам, не устанавливать на рабочие компьютеры не лицензионные программы. Соблюдение данных простых правил во многом поможет организации избежать «утечки» информации, и как следствие предотвратить возможные убытки.

Список использованных источников и литературы

1. Официальный сайт газеты «Комсомольская правда»
<https://www.kp.ru/guide/informatsionnaja-bezopasnost-predprijatija.html>
2. Официальный сайт компании «СерчИнформ»
<https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/>
3. Официальный сайт научно-исследовательского отдела информационной безопасности <http://www.cobra.ru/>
4. Официальный сайт компании «SafenSoft»
<http://rus.safensoft.com/security.phtml?c=768>
5. Официальный сайт Института судебных экспертиз и криминалистики <https://ceur.ru/news/921/item317493/>