Колотилина Мария Александровна

старший преподаватель

Уденцова Наталья Сергеевна

студентка

Соколова Ульяна Андреевна

студентка

ФГБОУ ВО «Самарский государственный экономический университет»

г. Самара, Самарская область

DOI 10.31483/r-75001

УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

***Аннотация:** в статье рассмотрены основные угрозы информационной безопасности, методы и средства по ее защите, проведен анализ угроз ИБ в корпоративных системах и изучены возможные пути решения по их устранению на примере ПАО «Сбербанк».*

***Ключевые слова:** информационная безопасность, корпоративная информационная система, вредоносные программы, проблема управления угрозами, несанкционированный доступ.*

В настоящее время фирму сложно представить без хорошо развитой корпоративной сети, обеспечивающей постоянный обмен деловой информацией независимо от местонахождения пользователей. Корпоративные информационные системы (КИС) стали важнейшим средством производства современной компании. Традиционные формы бизнеса они преобразовывают в электронную. Чтобы электронный бизнес существовал, нужна высокая защита корпоративной информации, а также поддержка инфраструктуры от случайных, а порой и преднамеренных воздействий, это и характеризует понятие «информационной безопасности». Она является одним из важнейших условий для существования такой формы бизнеса, так как ущерб от нарушения информационной безопас-

ности может привести не только к финансовым потерям, но даже к закрытию компании.

Вместе с появлением методов обработки, передачи и накопления информации, которые существуют на данный момент, стали появляться угрозы, которые приводят к потере, искажению и раскрытию данных, которые адресант отправляет конечному пользователю. Под угрозой безопасности информации подразумевают действия, которые способны прямо или косвенно нанести ущерб ее безопасности. Это может произойти и по ошибке сотрудников, и из-за попытки проникновения злоумышленников, и по техническим причинам, и даже по случаю стихийных бедствий, от которых никто не застрахован.

Несанкционированный доступ (НСД) считается самым распространенным видом компьютерных нарушений. Его суть состоит в том, что пользователь (нарушитель) получает доступ к объекту, нарушая при этом правила разграничения доступа, которые установлены в организации политикой безопасности. Распространенными приемами НСД являются [2, с. 3–4]:

- «маскарад», т. е. пользователь выполняет какие-либо действия от имени другого лица, обладающего определенными полномочиями;
- незаконное использование привилегий (нелегальный захват установленного системой защиты набора привилегий возможен из-за халатности администратора при назначении привилегий и управлении системой или при наличии ошибок в системе защиты);
- перехват паролей (специально разработанные программы пересылают владельцу программы-перехватчика данные, введенные законным пользователем при попытке входа в систему, в ходе чего нарушитель может использовать пароль и логин в своих целях) [5, с. 13].

Угрозу могут нанести и такие вредоносные программы, как компьютерные вирусы, программа «тройанский конь», сетевые «черви». Компьютерные вирусы способны заражать другие программы, изменяя их внедрением своей копии, которая может быть изменена (не исключено их дальнейшее размножение). Троянские программы распространяются людьми, причем они могут загружаться

непосредственно в компьютерные системы злоумышленниками, а также принуждать пользователей загружать и в дальнейшем запускать их на своих системах. Особенность этого вируса в том, что с виду он кажется безобидным файлом, который, на самом деле, представляет угрозу. И, наконец, сетевые «черви», распространяющиеся по глобальной сети, имеют цель попасть в систему, активироваться там и отправить свои копии другим пользователям, найденным на компьютере.

Борьба с этими вредоносными программами ведется с помощью разных антивирусных приложений, которые работают как на пользовательском уровне, так и на уровне сети. Однако, эти программы находятся в постоянном развитии, поэтому для эффективной борьбы с ними следуют обновлять программу защиты время от времени.

Возрастает распространенность непрограммных угроз. К ним относят следующее [5, с. 14–15].

1. Спам. Способен блокировать почтовые серверы, ограничивать доступ к информации, также может использоваться для распространения вредоносного программного обеспечения.

2. Фишинг – разновидность интернет-мошенничества, целью которой является заполучить личные данные пользователя (номера кредитных карт, банковских счетов, PIN-коды, пароли). Создав практические идентичные копии сайта банка и придумав причины, чтобы пользователь выдал конфиденциальные данные, злоумышленник таким образом втирается обманным путем к нему в доверие, и рассылает по электронной почте письма с помощью спам-технологии.

3. Фарминг – еще один вид мошенничества, с помощью которого можно получить данные пользователя через официальные веб-сайты путем фальсификации на серверах адресов настоящих веб-сайтов. В результате пользователь перенаправляется на сайт мошенника. Опасен фарминг тем, что отличить подделку практически невозможно.

Рассмотрим проблему обеспечения безопасности информационных систем с помощью двух подходов: фрагментарный и комплексный [4, с. 65–66].

Фрагментарный подход направлен противодействовать определенным угрозам в заданных условиях. С одной стороны, такие меры защиты информации полностью направлены на защиту только конкретных объектов информационной системы от определенных угроз, а с другой стороны, отсутствует единая защищенность среды обработки информации.

Комплексный же подход ориентирован на создание такой среды, которая защищает среду обработки информации в информационной системе, которая объединяет разные меры противодействия угрозам в единый комплекс. Сложность управления, настройки средств защиты, ограничение на свободу действий пользователей информационной системы являются недостатками данного подхода.

Для защиты корпоративных информационных систем больших компаний, которые обрабатывают особо важную информацию, применяют комплексный подход. Именно комплексную защиту они вынуждены реализовывать, так как нарушение безопасности информации в КИС крупных организаций может привести к огромному материальному ущербу и самой организации, и ее клиентам.

Изучением проблем управления угрозами информационной безопасности КИС и их устранения занимались многие специалисты. Например, А.М. Астахов в своей работе «Искусство управления информационными рисками» впервые ввел понятие профиль угроз. Существующие предпосылки в разработке профиля угроз, применение которого дает возможность построить систему управления ИБ предприятия, в свою очередь это позволит информации предприятия находиться под защитой [1, с. 7].

Одной из первых в России разработкой собственной системы информационной безопасности занялась банковская сфера в 90-х годах. Вся информация, которая хранится и обрабатывается в банковских организациях, подвергается рискам, связанным с разными вирусами, сбоями операционных систем и т. п. Если подобные угрозы информационной безопасности можно решить

путем ежедневного резервного копирования данных, то риски, связанные с несанкционированным доступом к конфиденциальной информации, требуют несколько иные пути решения. Рассмотрим применение некоторые из них на примере ПАО «Сбербанка».

Система защиты информации включает в себя элементы управленческого, ограничительного (режимного) и технологического характера, определяющие основные меры системы защиты, стимулирующие персонал соблюдать правила сохранения конфиденциальной информации фирмы. Естественно, организационные мероприятия должны быть четко регламентированы, спланированы и находиться под контролем службы информационной безопасности.

Существуют средства инженерно-технической защиты, включающие в себя [3]:

- физические средства, препятствующие доступу нарушителей на охраняемые объекты;
- средства защиты от утечки информации;
- средства по обеспечению охраны зданий и территории;
- средства обнаружения приборов и устройств технической разведки;
- технические средства контроля, предотвращающие вынос персоналом из помещения маркированных предметов, документов, книг и т. д.;
- средства предупреждения и защиты зданий от визуальных способов технической разведки.

Что же касается программно-аппаратной защиты конфиденциальной информации, которая хранится и обрабатывается в различных информационных системах, то здесь применяются средства выявления и защиты от НСД. К примеру, контроль за работой технических средств и сотрудников, использующих их, проверка обслуживания режимов обработки информации ограниченного пользования, защита операционных средств ЭВМ и программ пользователей и т. д.

Таким образом, для того чтобы данные, обрабатываемые в КИС, находились под защитой, необходимо обеспечивать корпоративные системы инфор-

мационной безопасностью, кроме того, не помешает своевременное обнаружение потенциальной угрозы нарушения ИБ. Эти меры способствуют безопасной работе организации.

Список литературы

1. Бабенко А.А. Модель профиля угроз информационной безопасности корпоративной информационной системы / А.А. Бабенко, С.С. Козунова. – Волгоград, 2018. – С. 7.
2. Горбачевская Е.Н. Исследование механизмов защиты данных в корпоративных информационных системах. – 2012.
3. Ханнанова Е.Н. Информационная безопасность Сбербанка России. – Магнитогорск, 2014. – 46 с.
4. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М.: ДМК Пресс, 2008. – 544 с.
5. Шаньгин В.Ф. Комплексная защита корпоративной информации. – 2009. – 196 с.