

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Колокина Евгения Михайловна

студент, магистрант, кафедра экономики организации производства

ФГБОУ «БГТУ им. В.Г. Шухова», г. Белгород

Развитие информационных технологий в современном обществе сделало компании зависимыми от информационных систем, а вместе с этим - уязвимыми к атакам хакеров, компьютерным вирусам, человеческому и государственному фактору настолько сильно, что многие владельцы бизнеса уже не могут чувствовать себя в безопасности. Вопрос информационной безопасности становится одним из наиважнейших в деятельности организации. Однако, это же развитие информационных технологий предлагает огромное множество решений, которые способны защитить данные от различных угроз. [5]

Что же такое информационная безопасность? Есть множество определений этого термина, вот некоторые из них:

- Информационная безопасность - это процесс обеспечения целостности, доступности и конфиденциальности информации.
- Информационная безопасность — состояние сохранности информационных ресурсов и защищенности, законных прав личности и общества в информационной сфере.
- Информационная безопасность — все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, подотчётности, доступности, неотказуемости, аутентичности и достоверности информации или средств её обработки. [2]

Под информационной безопасностью организации понимают следующее:

- защищенность информации и всей компании от намеренных или случайных действий, приводящих к нанесению ущерба ее владельцам или пользователям;
- состояние защищённости корпоративных данных, при которой обеспечивается их конфиденциальность, целостность, аутентичность и доступность. [1]

Обеспечение информационной безопасности организации в первую очередь должно быть направлено на предотвращение угроз, а не на ликвидацию их последствий. Именно принятие предупредительных мер по обеспечению конфиденциальности, целостности, а также доступности информации и является наиболее правильным подходом в обеспечении информационной безопасности организации.

Любая утечка информации из организации может привести к серьезным проблемам — от значительных финансовых убытков до полной ликвидации. Несомненно, проблема утечек информации появилась не только в эпоху бурного развития информационных технологий,

промышленный шпионаж и переманивание квалифицированных специалистов существовали еще задолго до этого. Но именно с появлением компьютера и интернета возникли новые методы незаконного получения информации.

Главными целями атак на информационные системы организаций являются:

1. получение контроля над ценными ресурсами (кража финансовой информации, эксплуатация вычислительных ресурсов корпоративной сети, кража различных баз данных);
2. ограничение деятельности предприятия по заказу недобросовестных конкурентов или политических оппонентов (вывод из строя информационной системы, разрушения связей с партнерами и т.д.). [6]

Современные компании сталкиваются с самыми разными угрозами информационной безопасности. Эти угрозы имеют как внутренние, так и внешние источники. К угрозам информационной безопасности организаций относятся:

1. Собственные сотрудники, их невнимательность и халатность (незлонамеренные нарушители). Непредумышленный урон конфиденциальным сведениям причиняется по простой халатности или невнимательности работников. Всегда есть вероятность того, что кто-нибудь из сотрудников откроет письмо с вирусом или вовсе занесет его с личного ноутбука на сервер компании. Так же угрозой является и то, что кто-либо из сотрудников может скопировать конфиденциальную информацию организации себе на флешку для удаленной работы. В такой ситуации информация является «легкой добычей».
2. Собственные злонамеренные сотрудники (инсайдеры). Угроза информационной безопасности исходит от сотрудников, которые умышленно крадут важную информацию за вознаграждение (преимущественно материальное) от компании-конкурента. Так же, утечка информации может осуществляться уволенными сотрудника, часто они забирают с собой всю информацию, к которой они имели доступ. Как правило, украденной информацией они пользуются на новом месте работы.
3. Использование нелегального программного обеспечения. Иногда, руководитель компании, в целях экономии средств устанавливает «пиратское» программное обеспечение. Поэтому, нелегальные программы не дают защиты от мошенников, заинтересованных в краже информации с помощью вирусов. Кроме того, при использовании нелегального программного обеспечения, компания не получает технической поддержки и своевременных обновлений, которые предоставляются компаниями-разработчиками.
4. Вирусы. На сегодняшний день, вирусы являются одной из самых опасных информационных угроз компании. Это объясняется тем, что появилось огромное

количество новых каналов проникновения вирусов. Наиболее уязвимым каналом по-прежнему остается электронная почта. Однако, с развитием информационных технологий, вирусы так же модифицировались. Теперь они способны проникать и через программы обмена сообщениями. Также, увеличилось и количество объектов для возможных вирусных атак.

5. Угрозы со стороны государства. В ходе проверок, государственные органы Российской Федерации имеют право конфисковать оборудование организации, а также носители информации. Так как, большая часть важных данных компании хранится в электронном виде на серверах, то при их изъятии, компания на какое-то время просто останавливает свою деятельность.
6. Стихийные бедствия. Пожары, наводнения, аварии в энергосистемах и т.д. Такая угроза очень опасна тем, что как правило, информацию восстановить практически невозможно. Кроме того, данную угрозу невозможно предвидеть. [3]

Несмотря на то, что количество угроз информационной безопасности постоянно растет, разработка средств защиты от них так же не стоит на месте и развивается. На практике применяются следующие средства защиты:

- Организационные средства (разработка внутренней документации, устанавливающая правила работы с компьютерной техникой и конфиденциальной информацией; проведение инструктажей и периодических проверок персонала; инициирование подписания дополнительных соглашений к трудовым договорам, где указана ответственность за разглашение или неправомерное использование информации, ставшей известной по работе; разграничение зоны ответственности, чтобы исключить ситуации, когда массивы наиболее важных данных находятся в распоряжении одного из сотрудников; организация работы в общих программах документооборота и слежение, чтобы критически важные файлы не хранились вне сетевых дисков; внедрение программных продуктов, которые защищают данные от копирования или уничтожения любым пользователем, в том числе топ-менеджментом организации; составление планов восстановления системы на случай выхода из строя по любым причинам);
- Технические средства (резервное копирование и удаленное хранение наиболее важных массивов данных в компьютерной системе - на регулярной основе; дублирование и резервирование всех подсистем сетей, которые имеют значение для сохранности данных; создание возможности перераспределять ресурсы сети в случаях нарушения работоспособности отдельных элементов; обеспечение возможности использовать резервные системы электропитания; обеспечение безопасности от пожара или повреждения оборудования водой; установка программного обеспечения, которое

обеспечивает защиту баз данных и другой информации от несанкционированного доступа; оборудование помещения камерами и сигнализацией);

- Аутентификация - это система способов проверки совпадения пользователя с тем образом, которому разрешен доступ;
- Идентификация - это механизм присвоения собственного уникального имени или образа пользователю, который взаимодействует с информацией. [4]

Подводя итог всего выше сказанного, можно сделать вывод, что защита информации должна осуществляться комплексно, сразу по нескольким направлениям. Чем больше методов будет задействовано, тем меньше вероятность возникновения угроз и утечки, тем устойчивее положение компании на рынке.

Список литературы:

1. Информационная безопасность предприятия: ключевые угрозы и средства защиты [Электронный ресурс] - Режим доступа. - URL: <https://www.kp.ru/guide/informatsionnaja-bezopasnost-predprijatija.html> - (дата обращения 20.03.2019)
2. Информационная безопасность [Электронный ресурс] - Режим доступа. - URL: <https://www.securitylab.ru/news/tags> - (дата обращения 20.03.2019)
3. Обеспечение информационной безопасности предприятия - [Электронный ресурс] - Режим доступа. - URL: <https://www.arinteg.ru/articles/informatsionnaya-bezopasnost-predpriyatiya-25799.html> - (дата обращения 20.03.2019)
4. Способы защиты информации [Электронный ресурс] - Режим доступа. - URL: <https://searchinform.ru/informatsionnaya-bezopasnost/zaschita-informatsii/sposoby-zaschity-informatsii/> - (дата обращения 20.03.2019)
5. Рябов, А. А. Математическое моделирование и алгоритмы оценки эффективности системы администрирования локальной компьютерной сети. / А.А. Рябов, В.А. Найденко // Моделирование, прогнозирование та інформаційно-аналітичне забезпечення інноваційного розвитку фінансової системи країни європейського простору: матеріали міжнарод. Наук.-практ. Конф. Молодих вчених та студентів 19 квітня 2012 року; Український державний університет фінансів та міжнародної торгівлі Харківський інститут фінансів УДУФМТ. - Х.: ХІФ УДУФМТ, 2012.-С. 590-592.
6. Рябов, А. А. Математическое моделирование производственной деятельности. / А.А. Рябов, А.Е. Десятова // Моделирование, прогнозирование та інформаційно-аналітичне забезпечення інноваційного розвитку фінансової системи країни європейського простору:

матеріали міжнарод. Наук.-практ. Конф. Молодих вчених та студентів 19 квітня 2012 року; Український державний університет фінансів та міжнародної торгівлі ; Харківський інститут фінансів УДУФМТ. - Х.: ХІФ УДУФМТ, 2012. - С. 577 - 580.