Vershkovich Anna, Matuloits Marina
Belarus state economic university

Problems and prospects of development of the land market in the Republic of Belarus

Annotation. In the article discusses the main problems and prospects of development of the land market in the Republic of Belarus, describes aspects of its reorganization.
Keywords: land market, forms of ownership, reorganization, land use optimization.

УДК 004

Войтов Дмитрий Александрович, Радченко Антон Михайлович
Белорусский государственный экономический университет
voytov.8@gmail.com anthony.by.ateo@gmail.com

Информационная безопасность

Данная работа является актуальной в связи с все большим развитиям информационных технологий, которые используются как государственными и коммерческими организациями, так и физическими лицами.

Целью исследования является выявления способов по защите информации, а также обнаружения основных каналов утечки данных.

Информационная безопасность — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации, вне зависимости от формы её представления (электронной или физической).

Объектами опасного информационного воздействия и информационной безопасности могут быть: сознание, психика людей; информационно-технические системы различного масштаба и назначения.

Средства обеспечения информационной безопасности - это средства, с помощью которых осуществляются меры по защите информации, систем управления, связи, компьютерных сетей, недопущению подслушивания, маскировке, предотвращению хищения информации.

Основные составляющие информационной безопасности:

Доступность – возможность за приемлемое время получить требуемую информационную услугу. Информационные системы создаются для получения определенных информационных услуг.

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций) [1].

Конфиденциальность – это защита от несанкционированного доступа к информации. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы [2].

Виды информационной безопасности, а точнее виды угроз защиты информации на предприятии подразделяются на пассивную и активную. Пассивный риск информационной безопасности направлен на внеправовое использование информационных ресурсов и не нацелен на нарушение функционирования информационной системы. К пассивному риску информационной безопасности можно отнести, например, доступ к базам данных или прослушивание каналов передачи данных. Активный риск информационной безопасности нацелен на нарушение функционирования действующей информационной системы путем целенаправленной атаки на ее компоненты. К активным видам угрозы компьютерной безопасности относится, например, физический вывод из строя компьютера или нарушение его работоспособности на уровне программного обеспечения.

Существует несколько групп методов защиты:

- Управление или влияние на элементы защищенной системы.
- Маскирование или преобразование данных с использованием криптографических методов.
- Регулирование или разработка законодательства и комплекс мер, направленных на поощрение надлежащего поведения пользователей, работающих с базами данных.
- Обеспечение соблюдения или создание условий, при которых пользователь будет вынужден соблюдать правила обработки данных.
- Поощрение или наращивание среды, которая мотивирует пользователей действовать должным образом.
- Препятствие предполагаемому нарушителю посредством физических и программных средств.

Основные методы защиты: организационные и технические средства.

Организационные средства:

Разработка организационных средств должна находиться в компетенции службы безопасности. Чаще всего эксперты по безопасности:

•Разрабатывают внутреннюю документацию, которая определяет правила работы с компьютерным оборудованием и конфиденциальной информацией.

•Предоставляют инструктаж и совершают периодические проверки персонала; инициируют подписание дополнительных соглашений к трудовым договорам, в которых излагаются обязанности по раскрытию или неправильному использованию связанной с работой информации.

•Лимитируют обязанности, чтобы избежать ситуаций, когда один сотрудник имеет в распоряжении самые важные файлы данных; организовывают работу с обычными рабочими приложениями и обеспечивают хранение важных файлов на сетевых дисках.

•Интегрируют программные продукты, которые защищают данные от копирования или уничтожения любым пользователем, включая высшее руководство компании.

•Разрабатывают планы восстановления системы в случае сбоев по любой причине.

Технические средства защиты:

•Дублирование и резервное копирование всех сетевых подсистем, которые важны для обеспечения безопасности данных.

•Возможность перераспределения сетевых ресурсов в случае сбоев отдельных элементов.

•Возможность использования систем резервного питания.

•Обеспечение безопасности от пожара или повреждения водой.

•Установка программного обеспечения, которое защищает базы данных и другую информацию от несанкционированного доступа.

•Регулярное резервное копирование и удаленное хранилище наиболее важных файлов данных в компьютерной системе.

Каналы утечки данных

Бумажные конфиденциальные документы могут быть выставлены чаще, независимо от характера утечки. Продажа секретов на бумаге более безопасна, чем в электронной форме, так как трудно доказать личность продавца (если нет записи).

Настольные компьютеры являются вторым наиболее распространенным каналом, который используется инсайдерами для

кражи конфиденциальной информации. Фактически, компьютер не является каналом для передачи конфиденциальных данных, а является каналом для его получения. С его помощью инсайдер может получить доступ к корпоративной информации на сервере компании, загрузить ее на съемный носитель или отправить по электронной почте.

Случайные утечки могут возникать, когда финансовые данные содержатся в онлайн-программах с простыми паролями. Это цифровые или алфавитные пароли по простому шаблону на клавиатуре. Сотрудники считают, что отправка конфиденциальных данных из личного окна более безопасна, чем из корпоративной почты. Это заблуждение, так как адрес электронной почты можно легко идентифицировать по учетным записям. Электронная почта также позволяет раскрывать секреты компании с вирусными письмами. Шпионы изучают интересы сотрудника (в социальных сетях и т. д.) И отправляют письмо, которое этот сотрудник, вероятно, откроет.

Смартфоны и ноутбуки являются менее распространенным каналом для утечки конфиденциальной информации, но они часто используются старшими менеджерами.

Таким образом, организационные и технические средства являются основными методами защиты информации, которые могут быть действенными, если используются в совокупности. Для защиты информации в компании необходима применять не только технические средства, но и организационные, потому что компания может подвергнутся атаками изнутри.

Источники литературы

1. Хрусталев, Е.В. Концептуальные основы построения системы информационной безопасности производственного предприятия / Е.В. Хрусталев, Елизарова М.И. // науч. журн. КубГАУ [Электронный ресурс]. – 2017. – №130(06). – Режим доступа: https://cyberleninka.ru/article/n/kontseptualnye-osnovy-postroeniya-sistemy-informatsionnoy-bezopasnosti-proizvodstvennogo-predpriyatiya. – Дата доступа: 28.11.2018.

2. Батаева, И.П. Защита информации и информационная безопасность / И.П. Батаева // Труды Межд. симпозиума «Надежность и качество» [Электронный ресурс]. – 2012. — Режим доступа: https://cyberleninka.ru/article/n/zaschita-informatsii-i-informatsionnaya-bezopasnost – Дата доступа: 28.11.2018.

Voytov Dmitry, Radchenko Anton
Belarus state economic university

Information security

Annotation. The article describes the main components of information security, methods for protecting information, methods of information leakage.

Key words: information security; protection of information; ways to leak information; information.