ORES
Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.056.53

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ, ФУНКЦИОНИРУЮЩЕЙ В СФЕРЕ СТРОИТЕЛЬСТВА

Лучинина Ольга Олеговна,
магистрант 3 курса, кафедра «Цифровые технологии и моделирование», Факультет заочного обучения ФГБОУ ВО «УГНТУ», г. Уфа
E-mail: olgyshka261@gmail.com

Аннотация

В данной статье рассматривается актуальный вопрос защиты информации в организациях, функционирующих в сфере строительства. В связи с тем, что данному вопросу в строительных организациях уделяют недостаточное внимание, существуют риски несанкционированного доступа к конфиденциальной информации, утечки или потери данных, которые могут привести к репутационным и финансовым потерям. Определены виды конфиденциальной информации, которая обрабатывается и накапливается в организациях.

Ключевые слова: система обеспечения информационной безопасности, защита информации, строительные организации, конфиденциальная информация.

ENSURING INFORMATION SECURITY OF AN ENTERPRISE OPERATING IN THE FIELD OF CONSTRUCTION

Olga O. Luchinina
3 rd year master's student, Department of «Digital technologies and modeling», Faculty of Correspondence Studies of the Federal State Budgetary Educational Institution of Higher Education «Ufa State Petroleum Technological University», Ufa
E-mail: olgyshka261@gmail.com

ABSTRACT

This article discusses the current issue of information security in organizations operating in the construction industry. Due to the fact that construction organizations pay insufficient attention to this issue, there are risks of unauthorized access to confidential information, leakage or loss of data, which can lead to reputational and financial losses. The types of confidential information that is processed and accumulated in organizations are identified.

Keywords: information security system, information protection construction organizations, confidential information.

Рост и развитие информационных технологий, а также отраслей, в которые данные технологии внедряются, ведет к существенному росту и разнообразию способов несанкционированного доступа к данным. Сфера строительства не является исключением.

Разнообразность информации, обрабатываемой и накапливаемой предприятиями, функционирующими в сфере строительства, становится причиной осуществления правонарушений.

В строительных организациях, как правило, основное внимание уделено качеству выполнения работ, качеству материалов, однако сфера защиты информации в таких организациях контролируется недостаточно. В связи с этим, недостаточная защита информации, используемой на предприятии может привести к серьезным убыткам, потери репутации и клиентов. Исходя из этого следует обеспечивать защиту информации на предприятиях, функционирующих в сфере строительства.

Защита информации осуществляется за счет реализации совокупности организационных и технических меры, которые направлены на минимизацию рисков возникновения несанкционированного доступа к информации, утечки или потери данных, а также обеспечения конфиденциальности, целостности и доступности информации.

Построение качественной и надежной системы обеспечения информационной безопасности (СОИБ) невозможно без определения структуры предприятия, выявления видов защищаемой информации, объектов защиты и построения модели угроз. На основании данных этапов формируются требования к проектируемой СОИБ, а затем она внедряется. Однако стоит отметить, что постоянно меняющиеся угрозы и технологии обязывают проектировать СОИБ с учетом этих изменений, а также вести непрерывную модернизацию уже имеющихся СОИБ. Это позволит организации адаптироваться к новым угрозам и обеспечивать эффективную защиту информации

Основными целями внедрения СОИБ являются [1]:

- предотвращение утечки, хищения, утраты, искажения, подделки информации вследствие ее тиражируемости;
- предотвращение угроз безопасности личности, предприятия, общества, государства вследствие разглашения или искажения информации;
- предотвращение несанкционированных действий по
- уничтожению, модификации, искажению, копированию, блокированию информации, что может привести к уменьшению ее потенциальной эффективности;
- предотвращение различных форм незаконного вмешательства в информационные ресурсы и системы предприятия;
- обеспечение правовой защиты информации как объекта собственности (исключение возможности ее незаконного тиражирования);
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах предприятий;
- сохранение конфиденциальности документированной информации в соответствии с законодательством (грифы секретности, прав доступа и распространения и т. д.).

Согласно Указу Президента РФ от 6 марта 1997 г. №188 «Об утверждении перечня сведений конфиденциального характера» [2] определены основные виды конфиденциальной информации, которые обрабатываются в строительных организациях:

- персональные данные (ПДн) (информация о персонале, о родственниках работников, о контрагентах – физических лицах);
- коммерческая тайна (КТ) (административная, финансовая, планово-экономическая, производственная и техническая информация, информация о контрагентах и партнерах, информация, касающаяся обеспечения безопасности).

Однако, для утверждения режима КТ должны быть разработаны и утверждены локальные документы организации, которые регулируются федеральным законом от 29.07.2004 №98-ФЗ «О коммерческой тайне» [3]:

- положение о КТ;
- перечень информации, составляющей КТ;
- дополнительные соглашения, подписываемые с работниками и с контрагентами;
- должностные инструкции ответственных за поддержание режима КТ;
- приказ «О назначении ответственных лиц»;
- приказ «Об утверждении перечня КТ»;
- приказ «Об утверждении перечня должностных лиц, допущенных к КТ».

Существует несколько методов, позволяющих обеспечить сохранность и защиту информации в строительной организации [4]:

- организационно-правовые;
- технические, которые в свою очередь подразделяются на: программные, физические, криптографические и аппаратные.

Таким образом, можно сказать, что система обеспечения безопасности информации в организации, функционирующей в сфере строительства, является очень важным аспектом, поскольку недостаточная защищенность данных может привести к серьезным последствиям. Ее создание, внедрение и поддержка требуют комплексного подхода и постоянного мониторинга. Однако, также важно учитывать специфические риски и особенности деятельности организации при разработке мер по обеспечению безопасности информации.

Список литературы:

1. Кожунова, Е. А. Обеспечение информационной безопасности на современном предприятии / Е. А. Кожунова // Школа Науки. – 2018. – № 2(2). – С. 19-21
2. Об утверждении перечня сведений конфиденциального характера : указ Президента РФ от 6.03.1997 №188 // Собрание законодательства РФ. – 1997. – № 10. – Ст. 1127.
3. О коммерческой тайне : федер. закон от 29.07.2004 №98-ФЗ (ред. от 14.07.2022) // Собрание законодательства РФ. – 2004. – № 32. – Ст. 3283 ; – 2022. – № 29. – Ст. 5278.
4. Аль-Аммори, А. Методы и средства защиты информации / А. Аль-Аммори, П.В. Дяченко, А.Е. Клочан, Е.В. Бакун, И.К. Козелецкая // The Scientific Heritage. – 2020. – №51-1. – С. 32-42.

References:

1. Kozhunova, E. A. Ensuring information security in a modern enterprise / E. A. Kozhunova // School of Science. – 2018. – No. 2(2). – pp. 19-21
2. On approval of the list of confidential information: decree of the President of the Russian Federation dated March 6, 1997 No. 188 // Collection of legislation of the Russian Federation. – 1997. – No. 10. – Art. 1127.
3. About trade secrets: federal. Law of July 29, 2004 No. 98-FZ (as amended on July 14, 2022) // Collection of legislation of the Russian Federation. – 2004. – No. 32. – Art. 3283; – 2022. – No. 29. – Art. 5278.
4. Al-Ammori, A. Methods and means of information security / A. Al-Ammori, P.V. Dyachenko, A.E. Klochan, E.V. Bakun, I.K. Kozeletskaya // The Scientific Heritage. – 2020. – No. 51-1. – P. 32-42.