УДК 33 DOI: 10.14451/1.242.353

Проблемы информационной безопасности в условиях цифровой трансформации

© 2025 **Юганова Мария Валентиновна**
Старший преподаватель кафедры Менеджмент, Санкт-Петербургский филиал Финансового университета при Правительстве РФ.
E-mail: mvyuganova@fa.ru

© 2025 **Нечаев Виктор Анатольевич**
Старший преподаватель кафедры Межкультурные коммуникации и общегуманитарные науки. Санкт-Петербургский филиал Финансового университета при Правительстве РФ.
E-mail: vanechaev@fa.ru

© 2025 **Нечаева Ольга Александровна**
Старший преподаватель кафедры Межкультурные коммуникации и общегуманитарные науки. Санкт-Петербургский филиал Финансового университета при Правительстве РФ.
E-mail: olanechaeva@fa.ru

© 2025 **Шепелева Ольга Петровна**
Кандидат сельскохозяйственных наук, доцент кафедры Бизнес-информатика. Санкт-Петербургский филиал Финансового университета при Правительстве РФ.
E-mail: shepelevaop@mail.ru

Ключевые слова: цифровая трансформация, программное обеспечение, информация, вредоносные программы.

Конфиденциальность, целостность и доступность информации, ее уязвимость и предотвращение атак вредоносных программ — главная задача организации любого масштаба. В современном мире, в котором стремительно развиваются информационные технологии, а также развивается зависимость от цифровых ресурсов, большая часть организаций переходит на формат современного обеспечения (электронные подписи, хранение данных на серверах, онлайн банки и т.д.). В связи с этим защита информационных систем (ЗИС) приобретает критическое значение.

Сложные, интегрированные комплексы аппаратных и программных средств, предназначенные для сбора, обработки, хранения, передачи и отображения информации. Основными признаками являются высокая степень автоматизации, что как раз-таки и позволяет компаниям и производствам отойти от старых форматов бумажной работы и огромного количества документов в архивах, как раз с помощью передовых технологий, таких как облачные хранения, обработка большого количества данных и искусственного интеллекта. ИС обеспечивает эффективное

управление информацией, автоматизацию процессов, а также помогает в принятии решений на основе данных.

Все это процессы и аспекты, которые в современном обществе крайне важны своей значимостью и полезностью, поэтому и существуют различные методы защиты информационных систем, без которых нашу жизнь сложно представить.

Эффективная ЗИС требует многогранного подхода, охватывающего различные уровни защиты:

1. Физическая безопасность: это защита физических компонентов системы от несанкционированного доступа, повреждений и кражи. Это подразумевает под собой охрану периметра определенным персоналом, использование камер видеонаблюдения, пропускных систем, чтобы никакой посторонний человек не мог попасть к охраняемым серверам и данным. Также существуют меры защиты оборудования от физических повреждений и краж (бронированное стекло, физические чип карты, с помощью которых открываются двери). Такой уровень защиты может показаться не настолько важным, но именно с этих аспектов и начинается защита информационных данных.
2. Защита от сетевых угроз: подразумевает под собой предотвращение нежелательного и несанкционированного доступа к системе через сеть. Ключевыми элементами защиты от проникновения является брандмауэры, которые фильтруют входящий и исходящий сетевой трафик, блокируя подозрительные соединения; системы обнаружения и предотвращения вторжений (IDS/IPS); VPN и механизмы защиты от DDoS- атак (это попытка злоумышленников при помощи вредоносных программ с множества устройств перегрузить сайт или приложение тем самым ограничить доступ пользователей к сайту и его приложениям).
3. Защита от вредоносного ПО: по сути своей это предупреждение возможных заражений систем от различных вирусов, троянов и других программ, несущих вред. Эффективными методами для того, чтобы защитить нашу систему является антивирусное ПО, эту структуру можно сравнить с нашим организмом, в который пытаются проникнуть болезни, но иммунная система с ним борется, но иногда не справляется и тогда приходят на помощь лекарства и витамины, таким же образом и антивирус укрепляет защиту системы от «болезней»; песочницы для безопасного запуска подозрительных файлов, а также регулярное обновление ПО, чтобы устранить уязвимости при помощи новейших драйверов.
4. Защита данных: достигнуть целостности, конфиденциальности и доступности данных можно путём использования шифрования данных (понять его смогут только пользователи для которых они предназначены), контроля доступа на основе ролей и прав пользователей (самым простым примером этого может служить логин и пароль для обычных юзеров приложения и отдельно для сотрудников осуществляющих тот самый контроль), резервного копирования и восстановления данных (как раз это и служит доступностью данных, чтобы они не были утеряны навсегда). Без всех этих пунктов компания не может существовать и давать уверенность в своей профессиональности своим клиентам.
5. Защита от социальных инженерных атак: это обучение сотрудников методам защиты от манипуляций злоумышленников: как предотвратить DDoS-атаку и восстановить работоспособность сайта, но основной атакой социальной инженерии помимо других, о которых с помощью повышения квалификации персонала улучшается их осведомлённость о них, является фишинговая атака, подразумевающая под собой получение идентификационных данных пользователей.
6. Аудит безопасности, управление уязвимостями и реагирование на инциденты: Регулярная проверка системы безопасности, идентификация и устранение уязвимостей позволяет разработать план реагирования на инциденты безопасности ЗИС и обработать

возможные атаки при помощи анализа логов (текстовый файл, куда автоматически записывается важная информация о работе системы, с помощью неё можно устранять неполадки и контроль работы), мониторинга системы.

Все эти аспекты существуют из-за столкновений информационных систем с постоянно эволюционирующими угрозами, таким как: увеличение сложности систем (более сложные системы сложнее защищать), появление новых типов атак, нехватка квалифицированных специалистов.

ЗИС является многогранной и постоянно развивающейся областью. Чтобы защита была эффективной требуется комплексный подход, охватывающий все аспект безопасности, начиная с физической безопасности организации заканчивая защитой данных и своевременным реагирование на инциденты. Качественная работа ЗИС невозможна без обучения и повышения квалификации сотрудников, а также адаптации к новым угрозам и типам атак от злоумышленников. Инвестиции в технологии безопасности — один из критических факторов в обеспечении надежной защиты в современном мире, так как для обеспечения надежности нужно обеспечить системы антивирусами достаточно хорошими, чтобы обезопасить данные, разработать методы для защиты от вредоносных атак, а также найти достаточно квалифицированных сотрудников и взрастить их в профессионалов, которые предотвратят любые попытки взлом и нарушения работы системы. Только комплексный подход, учитывающий как технические, так и организационные моменты, позволит обеспечить необходимый уровень безопасности и минимизировать риски и потери в использовании информационных систем.

Библиографический список

1. *Алборов Р. А.*, *Козменкова С. В.*, *Джикия К. А.* Совершенствование методики определения уровня существенности при планировании и проведении аудита // Бухучет в сельском хозяйстве. — 2024. — № 11. — С. 763—771.
2. *Амаду Х. М.* Проблемы определения уровня существенности аудита // Молодой ученый. — 2022. — 52(447). — С. 75—77.
3. *Богопольский А. Б.* Существенность в МСФО. — URL: https://www.cfin.ru/ias/msfo/cut_off_point.shtml (дата обр. 10.02.2025).
4. *Задонская К. С.* Категория существенности в аудите // Актуальные вопросы современной экономики. — 2022. — № 6. — С. 245—249.
5. *Захарченко К. А.* Методика расчета уровня существенности при проведении внутреннего аудита в торговой организации // Экономика и бизнес: теория и практика. — 2020. — 4—2(62). — С. 93—96.
6. *Захарченко К. А.*, *Пивень И. Г.* Методические подходы к определению существенности в аудите // Экономика и бизнес: теория и практика. — 2020. — № 4—2. — С. 97—100.
7. *Иванов А. Е.*, *Кресина А. М.* Оценка уровня существенности информации бухгалтерской финансовой отчетности при проведении аудита на основе анализа финансово-хозяйственной деятельности организации // Международный бухгалтерский учет. — 2019. — 30 (276). — С. 51—58.
8. *Кочинев Ю. Ю.* Численный анализ зависимости риска необнаружения в аудите от уровня существенности // Финансовый бизнес. — 2022. — 7(229). — С. 89—92.
9. *Шепелева О. П.*, *Кашин С. М.* Анализ теоретических положений о прикладном программном обеспечении для оптимизации и автоматизации бизнес-процессов организаций. — 2024.
10. *Шепелева О. П.*, *Полякова С. П.* Стратегическое управление устойчивостью интегрированной компании. — 2024.