УДК 004.056

Е.Д. КАНЗЮБА, студент гр. ЭРб-211 (КузГТУ)
Научный руководитель Т.М. ЧЕРНИКОВА, д.т.н., профессор (КузГТУ)
г.Кемерово

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КИБЕРУСТОЙЧИВОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ, АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Цифровизация общества, передача огромных объёмов данных через информационные и коммуникационные сети приводит к необходимости обеспечения для каждого из экономических субъектов информационной безопасность.

Информационная безопасность и киберустойчивость автоматизированных систем управления является определенным состоянием защиты информации и конфиденциальных данных от третьих лиц и внутренних пользователей без права авторизованного доступ к такой информации [1].

Целью инициатив по обеспечению информационной безопасности является именно информационная система, существующая внутри каждого из действующих хозяйствующих субъектов в современной цифровой экономике.

Информационные и коммуникационные системы по своему составу и структуре автоматизированных систем управления, подвержены угрозам безопасности, они очень похожи друг на друга и содержат следующие главные элементы.

1. Информационные ресурсы как первичное хранилище информации в форме баз данных, информаций, накопленных знаний об объекте либо явлении. Отношения между отдельными элементами информационных ресурсов определяются конкретными алгоритмами и установленными правилами разработчика этой информационной системы [2].

2. Программные модули, также созданные разработчиком информационной системы, главной функциональной задачей которых является предоставление пользователю возможности ввода данных, а затем автоматическая обработка этих данных, поиск и формирование отчета о поиске данных и сведений из этой системы.

3. Интерфейс, основная задача которого – обеспечить наиболее удобное, наглядное и эффективное взаимодействие пользователя с информационной системой. Зачастую именно характеристики интерфейса,

его качество и актуальность улучшают уровень спроса на информационную систему со стороны конечного потребителя.

4. Персонал, являющийся пользователем информационной системы. Как правило, автоматизированные информационные системы создаются для корпорации, организации и государственных учреждений, для автоматизации действий, упрощений задач, возможности хранения и систематизации больших объёмов данных. Но, например, некоторые информационные системы, такие как электронно-правовые модули Консультант Плюс или Гарант могут быть ориентированы на индивидуального пользователя – физическое лицо.

Исходя из этого, можно заключить следующее: информационные системы разрабатываются под решение поставленных задач, определяемых функциональным аспектом пользователей данного электронного продукта. Система защиты данных – структура информационной системы против несанкционированного доступа, она также поддерживает соответствующий уровень информационной безопасности.

5. Ряд технических средств, в том числе прямая компьютерная сеть, устройства, обеспечивающие прием данных, и процессоры для передачи, обработки информации и многих других форм, оборудование и технические системы в войсковых соединениях. Комплекс технической и электронной поддержки функций информационные системы.

Решение вопросов обеспечения информационной безопасности и киберустойчивости автоматизированных систем управления осуществляется сотрудниками IT-отделов и специализированных учреждений, работающих на контрактной основе, они участвуют в организации, обеспечении надлежащего уровня защиты информации от кражи, воздействия вредоносных вирусов.

Инструменты и методы защиты информационных систем тесно взаимосвязаны и определяются общими мерами информационной безопасности, помимо предотвращения несанкционированной утечки.

Рассматривая целостность применения всех таких средств и методов информационной защиты как системную конструкцию отмечаем, что информационная безопасность и киберустойчивость предполагает построение рационального, технически продуманного и апробированного механизма снижения уязвимости информации, создание барьеров для беспрепятственного доступа к ней посторонних лиц, не обладающих соответствующими правами.

Поэтому в качестве мер по улучшению обеспечения безопасности и киберустойчивости предлагается обеспечение защиты по трём группам.

Группа 1 – правовая защита информации.

Данный инструмент информационной безопасности основывается на правовых нормах в области информационных технологий и телекоммуникаций, которые регулируют отношения между пользователями и получателями информации. Правовая защита в информационных системах организации включает в себя следующие действия:

- включение норм об ответственности за разглашение конфиденциальной информации в должностные инструкции, трудовые договоры с работниками, а также в соглашения и договоры, заключаемые организацией;
- информирование всех сотрудников о правовых последствиях несанкционированной передачи информации из информационной системы третьим лицам;
- организация и проведение собраний персонала с целью информирования сотрудников о недопустимости передачи информации и документов из информационных систем и электронного документооборота компании третьим лицам без согласования с руководством.

Группа 2 – инженерно-техническая защита.

Данные меры по обеспечению безопасности при использовании информационных систем компании в настоящее время разнообразны по содержанию и функциональному назначению.

К таким мерам относятся аппаратные средства, реализующие генераторы помех, сетевые фильтры, препятствующие подключению сторонних пользователей к сети связи, а также использование автоматизированных систем управления.

Практическим решением при разработке систем защиты информации является метод аутентификации [3].

До начала дальнейшей работы над информационными системами, которые предлагается внедрить для повышения уровня информационной безопасности, используются три основных вида аутентификации пользователей:

- использование паролей и ключей шифрования;
- аутентификация на основе имеющейся информации электронных ключей о соответствующем пользователе;
- аутентификация по биометрическим данным (например, голос, отпечаток пальца).

Важным элементом технической защиты информации и документов в информационной системе является бесперебойное электропитание серверов и меры безопасности, связанные с рабочими компьютерами сотрудников. Для этих целей на практике используются источники

бесперебойного питания. Источники бесперебойного питания могут поддерживать работу оборудования предприятия в течение определенного времени для создания резервных копий информации [4].

Группа 3 – организационная защита информации в информационных системах.

К этой группе относятся все действия руководства коммерческих предприятий, связанные с организацией процессов, обеспечивающих всем сотрудникам возможность входа и работы в информационных системах. Для этих целей привлекается техническое оснащение помещений и создание необходимых коммуникаций. Конкретный перечень организационных мер по защите информации определяется спецификой учреждения, формой его деятельности и объемом информации и электронных документов, которыми обмениваются в информационной системе.

Достоинство организационных методов защиты информации заключается в однонаправленности действий, которые могут постоянно изменяться, исходя из новых ситуаций и проблем. Недостатком таких организационных методов является их зависимость от субъективных факторов, которые могут отличаться в различных функциональных бизнес-системах предприятия.

Список литературы:

1. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. – Москва: Риор, 2021. - 400 с.

5. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2020. - 324 с.

3. Голицына, О.Л. Информационные системы: Учебное пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов. – М.: Форум, 2019. – 352 с.

4. Глущенко, И.С. Современные информационные системы анализа и управления рисками в сфере информационной безопасности / И.С. Глущенко // Известия ТулГУ. Технические науки.– 2021.– №2. - С. 24-28.

Информация об авторах:

Канзюба Евгений Дмитриевич, студент гр. ЭРб-211, КузГТУ, 650000, г. Кемерово, ул. Весенняя, д. 28, ked13077@list.ru

Черникова Татьяна Макаровна, д.т.н., профессор, КузГТУ, 650000, г. Кемерово, ул. Весенняя, д. 28, chtm.oe@kuzstu.ru