Секция «Управление бизнесом в цифровой экономике»

Управление кибернетической и информационной безопасностью в системах электронного документооборота

Научный руководитель – Коробейникова Кристина Валерьевна

Коробейникова Кристина Валерьевна
Кандидат наук
Донецкий национальный университет, Факультет математики и информационных технологий, Кафедра информационных систем управления, Донецк, Украина
E-mail: k.korobeinikova@donnu.ru

Коробейникова Кристина Валерьевна
Доцент, кандидат экономических наук
ГОУ ВПО «Донецкий национальный университет», факультет математики и информационных технологий, Донецк, Донецкая Народная Республика
E-mail**:** k.korobeinikova@donnu.ru

Актуальность решения проблем кибернетической и информационной безопасности электронного документооборота (ЭДО) обусловливается стремительным развитием информационных технологий, информатизацией и компьютеризацией различных сфер человеческой деятельности.

В работах ряда ученых, таких как Д. Н. Карпов, М. Д. Колотырин, А. А. Рублевская, В. Н. Махалин и др., раскрываются особенности различных направлений обеспечения кибербезопасности. При этом вопросы защиты информации в ЭДО в указанных работах не нашли должного отображения, что побуждает к продолжению исследований в данной научной области.

Под кибербезопасностью в системах ЭДО понимается желаемое состояние информационной системы, позволяющее ей противостоять воздействиям из киберпространства, которые могут поставить под угрозу доступность, целостность или конфиденциальность данных, которые сохраняются, обрабатываются или передаются в системах электронного документооборота (СЭД), и связанных с ними процессов и документов [1].

С другой стороны, кибербезопасность - это совокупность усилий по предотвращению вреда, в том числе с использованием правовых средств, который может быть причинен в результате сбоев в работе информационно-компьютерных систем (ИКТ) или неправильного их использования, а также по восстановлению ИКТ после реализации этих угроз [2].

Анализ существующих тенденций развития компьютерных атак, создающих угрозы для кибернетической и информационной безопасности в ЭДО, свидетельствует, что сегодня, как правило, последние направлены на:

- выведение из строя информационных систем с помощью вредоносного ПО;
- временное блокирование информационных систем и публичных web-сайтов, объектов критической инфраструктуры путем массированных кибератак;
- незаконное получение конфиденциальных данных.

Резкий рост количества кибератак злоумышленников на системы управления, в том числе на системы ЭДО государственных учреждений, стал глобальной ключевой проблемой современности. В связи с этим важно выяснить причины возникновения и технологии осуществления киберпреступлений, без чего невозможно разработать меры кибербезопасности.

Одной из существенных проблем применительно к ЭДО является обеспечение конфиденциальности данных в СЭД. Любая СЭД, которая имеет средства обеспечения безопасности, должна, в частности, предусматривать механизмы безопасного доступа к системе, механизмы защиты от основных киберугроз, направленных против обеспечения сохранности документов, их подлинности, а также механизмы протоколирования пользователей в системе.

Анализ угроз в сфере кибербезопасности позволяет предположить, что дальнейшее развитие обеспечение кибербезопасности в ЭДО будет осуществляться путем регламентации процедур:

- аутентификации пользователя системы (учитывалось также количество уровней аутентификации);
- распределения прав доступа для пользователей системы;
- подписания документов с использованием средств электронной подписи;
- шифрования данных;
- протоколирования и аудита работы пользователей в системе;
- резервного копирования

На российском рынке широко используются такие программные продукты, как «Логика Бизнеса», ЭОС, «Ланит», «Интертраст», Docvision, Directum, ELMA ECM+, Optima WorkFlow, «1С: Документооборот». Сравнительный анализ показывает, что во всех СЭД предусмотрены процедуры аутентификация пользователей, разграничение прав доступа, поддержка электронной подписи, возможность шифрования данных, протоколирование и аудит работы пользователей в системе. Во всех СЭД, кроме «1С: Документооборот» имеются средства резервного копирования и восстановления.

Проведенные ранее исследования показывают, что большая часть угроз в области ЭДО направлена на внедрение и выполнение произвольного кода, в том числе с помощью специально сформированных BMP-изображений. Это позволяет злоумышленникам оказывать воздействие на целостность защищаемой информации с помощью специально созданного web-запроса, узнавать имя последнего авторизовавшегося пользователя, получать доступ к любой учетной записи, определять все существующие имена пользователей, используя метод полного перебора имен в поле username, с помощью специально сформированных POST-запросов.

Для отказа в обслуживании системы используются также специально сформированные электронные письма или документы Office, которые содержат код, позволяющий нарушителю обойти систему обнаружения вируса или спама и получить несанкционированный доступ к защищаемой информации и к криптографическим ключам.

Анализ основных уязвимостей безопасности СЭД, представленный на сайте ФСТЭК России, показал, что в качестве киберугроз могут рассматриваться действия злоумышленников, в том числе сотрудников организации, которые стремятся повысить свои привилегии при доступе к СЭД с применением кибератак. Нарушение правил разграничения доступа позволяет им получить доступ к защищаемой информации.

В связи с этим представляется актуальным представляется целесообразным закрепить требования к аутентификации пользователей и разграничению полномочий, а также ответственность за совершение действий типа «полный перебор» (brute force), который может привести к нарушению безопасности и целостности СЭД.

Источники и литература

1) 1. Анискин С. С., Селедцов В. Ю. Кибербезопасность как один из трендов цифровой экономики России // Образование и наука без границ: социально-гуманитарные науки. – 2019. № 12. С.28-31
2) 2. Литвинов Д. А. Оценка политики России в области кибербезопасности и возможные варианты ее совершенствования // Вестник науки и образования. 2019. № 19 2 (73). С. 76–82