Анализ угроз ЛОЦМАН: PLM в конструкторском бюро

С.С. Козунова,
асп. каф. САПРиПК, one1100on@gmail.com,
А.Г. Кравец,
проф. каф. САПРиПК, д.т.н, проф., agk@gde.ru,
ВолгГТУ, г. Волгоград

В докладе исследуются угрозы нарушения информационной безопасности системы ЛОЦМАН: PLM в конструкторском бюро. Угрозы проанализированы по «источнику», исходя из структуры ЛОЦМАН: PLM и корпоративной сети. Описан ущерб конструкторского бюро, к которому может привести реализация угроз.

The report explores threats of information security breach of the LOTSMAN:PLM system in the design department. Threats are analyzed by the "source", proceeding from the structure of the LOTSMAN:PLM and the corporate network. The damage to the design department, to which the implementation of threats may lead, was described.

Введение

Одним из самых востребованных направлений в автоматизации деятельности конструкторского бюро (КБ) является использование системы управления инженерными данными и жизненным циклом изделия ЛОЦМАН: PLM. Однако при вводе в эксплуатацию ЛОЦМАН: PLM специалисты КБ сталкиваются с проблемами обеспечения надёжности и информационной безопасности (ИБ) такой системы [1]. Открытыми являются следующие вопросы: категорирование информации, обрабатываемой в ЛОЦМАН: PLM, и управление угрозами ИБ. Стоит отметить, что если КБ не является обособленным и входит в состав промышленного предприятия, например, оборонно-промышленного комплекса (ОПК), то ЛОЦМАН: PLM является информационной системой (ИС) управления производством.

Актуальность исследуемой области обосновывают незначительное число исследований проблемы анализа угроз ЛОЦМАН: PLM в КБ и необходимость выполнения требований КБ ФЗ от 26.07.2017 №187 «О безопасности критической информационной инфраструктуры РФ».

1. Структура и описание ЛОЦМАН: PLM

Система управления инженерными данными и жизненным циклом изделия ЛОЦМАН: PLM позволяет оптимизировать обработку конструкторской документации. Структура такой системы представляет собой клиент-серверное приложение, состоящее из средства конфигурации и администрирования, а также следующих прикладных модулей: извещение, архив, технология, импорт-экспорт, обмен данными. Удобство применения ЛОЦМАН: PLM в КБ обеспечивают функции управления процессами, структурой и конфигурациями изделиями, хранением данных и документов.

Таким образом, ЛОЦМАН: PLM можно рассматривать как сложную систему [2], которая позволяет создавать подсистемы управления данными с учётом специфики КБ [3] (см. рис. 1).

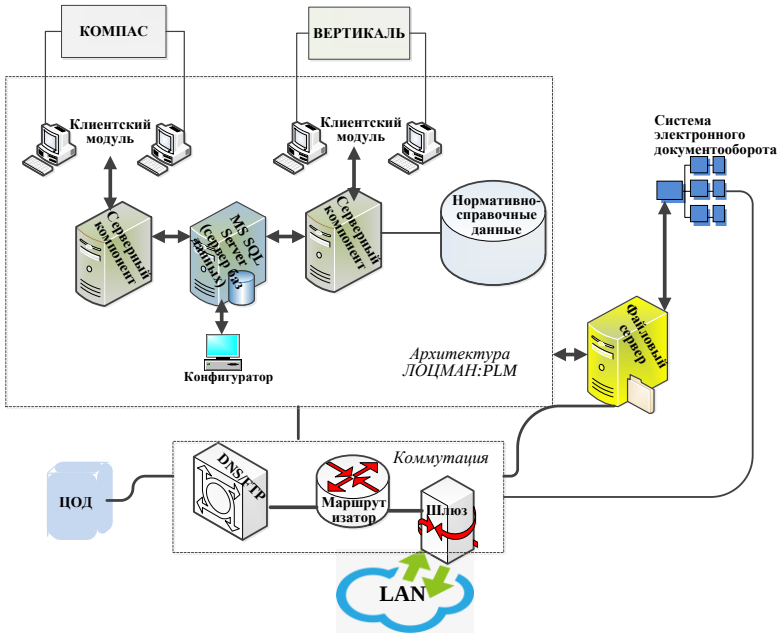

рис. 1 Типовая инфраструктура корпоративной сети конструкторского бюро с интеграцией ЛОЦМАН: PLM

2. Общая характеристика проблемы анализа угроз информационной безопасности ЛОЦМАН: PLM

Вопросы обеспечения ИБ и надёжности информационных систем изучаются достаточно давно, однако проблематики ИБ и надёжности ЛОЦМАН: PLM исследуются сравнительно недавно. В настоящее время не существует мето-

дов и подходов, позволяющих решить частную задачу анализа угроз для сложных систем, а также учитывающую специфику КБ [7]. Поэтому с практической точки зрения остаётся только руководствоваться методикой ФСТЭК [8] и исполнять требования [9], однако этого недостаточно для проведения комплексного анализа угроз ИБ ЛОЦМАН: PLM, а также для прогнозирования ущербов. Сказанное выше, а также импортозамещение конструкторского и инженерного программного обеспечения актуализируют необходимость анализа угроз ИБ ЛОЦМАН: PLM в КБ.

3. Угрозы информационной безопасности ЛОЦМАН: PLM

При формировании модели угроз ИБ какой-либо ИС, основополагающим является процедура анализа угроз, предназначенная для выявления актуальных угроз ИБ с целью последующей разработки сценариев нарушителей.

Проанализировав стандартизированные методики [4,5], в которых изложены основная терминология ИБ, можно сделать вывод о взаимосвязи между угрозами, источниками, уязвимостями и атаками. Исходя из этого, а также основываясь на банке данных угроз безопасности информации ФСТЭК России [6], опишем угрозы ИБ, характерные для ЛОЦМАН: PLM (таблица 1).

Таблица 1

Описание угроз информационной безопасности ЛОЦМАН: PLM

№	Тип угрозы	Угрозы	Источник угроз
1	Угрозы несанкционированного доступа	Кража (утеря) носителей информации; Несанкционированный доступ к информации, хранящейся на съемных машинных носителях информации; Восстановление защищаемой информации и информации о ЛОЦМАН: PLM путем анализа содержимого носителей информации; Несанкционированный доступ к КД, обрабатываемой в ЛОЦМАН: PLM; Модификация, уничтожение, блокирование информации; Нарушение работоспособности клиентского модуля ЛОЦМАН: PLM или АРМ пользователя корпоративной сети КБ; Нарушение работоспособности коммутационного оборудования, каналов связи корпоративной сети КБ; Несанкционированное (в том числе непреднамеренное) отключение средств защиты информации; Внедрение вредоносного программного обеспечения; Проведение атак, основанных на использовании уязвимостей программных средств корпоративной сети КБ и ЛОЦМАН: PLM; Модификация КД.	Непосредственный физический доступ к техническим средствам корпоративной сети или ЛОЦМАН: PLM, который может быть осуществлён внутренним нарушителем (или внешним, находящимся на территории КБ)
2	Угрозы, осуществляемые с использованием протоколов межсетевого взаимодействия	Разглашение информации путем передачи ее по электронной почте, системам обмена моментальными сообщениями и т.п.; Анализ сетевого трафика с перехватом передаваемой из ЛОЦМАН: PLM и принимаемой в корпоративной сети из внешних сетей информации; Получение сведений об программно-аппаратных средствах ЛОЦМАН: PLM путем прослушивания каналов связи; Создание нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных; Отказ в обслуживании; Подбор, взлом паролей к доменным учётным записям пользователей, а также к пользовательским и техническим учётным записям ЛОЦМАН: PLM; Навязывание ложного маршрута путем несанкционированного изменения маршрутно-адресных данных внутри корпоративной сети;	Неограниченная программная среда; Аппаратное обеспечение; Среда виртуализации; Избыточность сетевых протоколов; Ошибки доступа к данным; Некорректная обработка входных данных

		Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ЛОЦМАН: PLM, топологии сети, открытых портов и служб, открытых соединений	
3	Угрозы нарушения надёжности	Отсутствие в КБ системы резервного копирования и восстановления данных; Не реализовано резервное копирование базы данных ЛОЦМАН: PLM встроенными инструментами MS SQL Server; Некорректное конфигурирование систем аппаратной виртуализации, резервного копирования и восстановление данных; Иные дефекты конфигурирования ЛОЦМАН: PLM, допущенные при вводе в эксплуатацию и техническом сопровождении; Некорректное использования системы мониторинга.	Стихийные источники потенциальных угроз, являющимися внешними; Источники, связанные с техническими средствами корпоративной сети, и ЛОЦМАН: PLM, являющимися внутренними

Таким образом, для ЛОЦМАН: PLM характерно три типа угроз: угрозы несанкционированного доступа; угрозы, осуществляемые с использованием протоколов межсетевого взаимодействия; угрозы нарушения надёжности. Первый тип угроз способен привести к нарушению конфиденциальности, целостности и доступности КД – комплексности организации КД об изделии и процессах обеспечения доступа к ней; недоступности задания на проектирования исходной документации. Второй тип может нанести такой ущерб как: экономический и репутационные ущербы, кража КД и попадание коммерческой тайны третьим лицам, а также приостановление обмена заданиями между подразделениями КБ. Третий тип угроз влечёт за собой следующие последствия: частичное или полное прекращение функционирования ЛОЦМАН: PLM, корпоративной сети КБ и приостановление бизнес-процессов [7].

Заключение

Анализ угроз ИБ ЛОЦМАН: PLM позволяет поддерживать в актуальном состоянии списки угроз ИБ для ЛОЦМАН: PLM, а также прогнозировать ущерб и атаки. Опираясь на результаты исследований, изложенных авторами в данном докладе, можно разработать метод и алгоритм количественной оценки и управления угрозами ИБ ЛОЦМАН: PLM в КБ. Перспективой развития данного исследования является разработка сценариев злоумышленника ИБ и моделирование атак на ЛОЦМАН: PLM и корпоративную сеть КБ.

Литература

1. Kravets A. The Risk Management Model of Design Department's PDM Information System / А.Г. Кравец, С.С. Козунова // Creativity in Intelligent Technologies and Data Science. Second Conference, CIT&DS 2017 (Volgograd, Russia, September 12-14, 2017): Proceedings (Ser. Communications in Computer and Information Science. Vol. 754) / ed. by A. Kravets, M. Shcherbakov, M. Kultsova, Peter Groumpos. Volgograd State Technical University [et al.]; [Germany]: Springer International Publishing AG, 2017. P. 490–500.
2. Павловский И.С. Концептуальные исследования проблемы интеграции систем управления технологическими процессами // XV – международная молодёжная конференция «Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта CAD/CAM/PDM – 2015». URL: http://lab18.ipu.ru/projects/conf2015/1/8.htm (дата обращения: 10.09.2018).
3. Кондратьев С.Е., Ульянин О.В., Абакумов Е.М. Совершенствование процессов обмена данными между PLM-системой и корпоративной информационно-управляющей системой в интегрированной информационной среде // XV – международная молодёжная конференция «Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта CAD/CAM/PDM – 2015». URL: http://lab18.ipu.ru/projects/conf2015/3/11.htm (дата обращения: 11.09.2018).
4. ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. – М: Стандартинформ, 2014 г.
5. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – М: Стандартинформ, 2011 г.
6. Банк данных угроз безопасности информации ФСТЭК России. URL: https://bdu.fstec.ru/threat (дата обращения: 10.09.2018).
7. Система управления информационной безопасностью документооборота на предприятии / В.Ю. Шевцов, А.А. Бабенко, С.С. Козунова, А.Г. Кравец // Прикаспийский журнал: управление и высокие технологии. - 2018. - № 1 (41). - С. 161-172.
8. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. зам. директора ФСТЭК России 14 февраля 2008 г.). URL: https://fstec.ru/component/attachments/download/290 (дата обращения: 11.09.2018).
9. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ ФСТЭК России от 11 февраля 2013 г. № 17 (ред. от 15.02.2017). URL: http://fstec.ru/component/attachments/download/567 (дата обращения: 11.09.2018).