УДК 004.056.5 + 005.92:004.63.056 Вестник УрФО № 4(26) / 2017, с. 12–15

Басыров Р. Р., Паршин К. А.

АНАЛИЗ ВЗАИМОСВЯЗИ УГРОЗ И УЯЗВИМОСТЕЙ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

В статье проводится анализ взаимосвязи уязвимостей и угроз информационной безопасности в современных информационных системах электронного документооборота. Рассматриваются основные специфичные процессы обработки информации в системах электронного документооборота. Определены зависимости между процессами по обработке информации, влияющие на защищенность информации в системах ЭДО. На основании проведенных исследований разработана математическая модель вероятности реализации угроз информационной безопасности в зависимости от вероятности реализации той или иной уязвимости. Дана оценка защищенности современных систем ЭДО.

Ключевые слова: *документ, информация, информационная безопасность, угроза, уязвимость, документооборот, реквизит, защита информации, система электронного документооборота.*

Basyirov R. R., Parshin K. A.

ANALYSIS OF THE RELATIONSHIP BETWEEN THREATS AND VULNERABILITIES IN ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

The article analyzes the correlation of vulnerabilities and threats to information security in modern information systems of electronic document management. The main specific processes of information processing in electronic document management systems are considered. Dependencies between information processing processes affecting the security of information in EDM systems have been determined. Based on the conducted research, a mathematical model of the probability of implementing information security threats has been developed, depending

on the likelihood of the implementation of a particular vulnerability. The evaluation of the security of modern EDM systems is given.

Keywords: *document, information, information security, threat, vulnerability, document circulation, props, information protection, electronic document management system.*

В связи с бурным информационным развитием общества и производства, в большинстве государственных, муниципальных учреждений, а также многих крупных коммерческих организациях внедряются системы электронного документооборота. Данные системы позволяют разгрузить бюрократическую машину в организации, повысить темпы работы по обработке информации содержащейся в документах, предоставить мобильный доступ к документам, повысить трудовую дисциплину сотрудников за счет автоматизированных средств контроля работы с документами.

Однако при всех положительных результатах использования систем электронного документооборота, возникают угрозы информационной безопасности, присущие всем автоматизированным информационным системам. Таким образом, определение взаимосвязи угроз безопасности информации, хранящейся и обрабатываемой в СЭД, позволит создать эффективную методику использования методов и средств защиты информации для достижения необходимого уровня защищенности системы.

Для реализации поставленной задачи, в первую очередь, необходимо определить основные процессы по обработке информации, протекающие в электронном документообороте. Согласно определению, процесс документооборота заключается в движение документов в организации с момента их создания или получения до завершения исполнения или отправки[1]. Таким образом можно выявить основные процессы обработки информации, протекающие в документообороте:

1) создание документа;

2) получение документа;

3) исполнение документа;

4) отправка документа;

Проведя анализ информационных потоков и информации, обрабатываемой в данных процессах, можно выделить следующие информационные группы:

1 – Содержание документа;

2 – Реквизиты документа;

3 – Информация о согласовании документа;

4 – Информация об исполнении документа;

Отметим, что информация, относящаяся к 1 и 2 группе, является обязательной и без неё электронный документ не может существовать. Информация из 3 и 4 группы может отсутствовать в документе, но при её наличии непосредственно характеризует информацию из 1 и 2 группы.

Для информации относящееся любой из этих групп характерны следующие уязвимости, нарушающие состояние защищенности: нарушение конфиденциальности, нарушение целостности, блокирование доступности информации, содержащейся в электронном документе. Введем условное обозначение для таких уязвимостей: V_n^m, где V – уязвимость, нарушающее состояние защищенности информации, относящейся к *n = 1...4* группе, в результате применения *m = к, ц, д* воздействия.

Изучив рынок современны систем электронного документооборота, проведя анализ технологии формирования информационных потоков в таких системах и учитывая взаимосвязь информационных групп, были сделаны выводы о взаимосвязи уязвимостей и угроз, возникающих в результате их реализации. Вероятность возникновения события $P(T_n^m)$, нарушающего состояние защищенности информации, характеризуется вероятностью использования уязвимости и/или совокупности уязвимостей[2,3].

Далее выведены формулы для расчета вероятностей возникновения угроз в СЭД для каждой информационной группы в зависимости от реализованных уязвимостей.

Вероятности угрозы нарушения конфиденциальности информации:

$$P(T_1^к)=P(T_1^к|V_2^ц)*P(V_2^ц)+P(T_1^к|V_3^к)*P(V_3^к)+P(T_1^к|V_4^к)*P(V_4^к) \quad (1)$$

$$P(T_2^к)=P(T_2^к|V_2^ц)*P(V_2^ц)+P(T_2^к|V_3^к)*P(V_3^к)+P(T_2^к|V_4^к)*P(V_4^к) \quad (2)$$

$$P(T_3^к)=P(T_3^к|V_2^ц)*P(V_2^ц)+P(T_3^к|V_3^к)*P(V_3^к) \quad (3)$$

$$P(T_4^к)=P(T_4^к|V_2^ц)*P(V_2^ц)+P(T_4^к|V_4^к)*P(V_4^к) \quad (4)$$

Вероятности угрозы нарушения целостности информации:

$$P(T_1^ц)=P(T_1^ц|V_2^ц)*P(V_2^ц)+P(T_1^ц|V_1^ц)*P(V_1^ц) \quad (5)$$

$$P(T_2^ц)=P(V_2^ц) \quad (6)$$

$$P(T_3^ц)=P(T_3^ц|V_2^ц)*P(V_2^ц)+P(T_3^ц|V_2^ц)*P(V_3^ц) \quad (7)$$

$$P(T_4^ц)=P(T_4^ц|V_2^ц)*P(V_2^ц)+P(T_4^ц|V_2^ц)*P(V_4^ц) \quad (8)$$

Вероятности угрозы нарушения доступности информации:

$$P(T_1^д)=P(T_1^д|V_2^ч)*P(V_2^ч)+P(T_1^д|V_1^ч)*P(V_1^ч) \quad (9)$$

$$P(T_2^д)=P(T_2^д|V_2^ч)*P(V_2^ч)+P(T_2^д|V_2^д)*P(V_2^д) \quad (10)$$

$$P(T_3^д)=P(T_3^д|V_2^ч)*P(V_2^ч)+P(T_2^д|V_3^ч)*P(V_3^ч)+P(T_2^д|V_3^д)*P(V_3^д) \quad (11)$$

$$P(T_4^д)=P(T_4^д|V_2^ч)*P(V_2^ч)+ P(T_2^д|V_4^ч)*P(V_4^ч)+P(T_2^д|V_4^д)*P(V_4^д) \quad (12)$$

Исходя из рассмотренных вероятностей, следует выделить уязвимость нарушения целостности реквизитов документа $P(V_2^ч)$, так как именно реквизиты документа определяют права пользователей на работу с документами. Иными словами, изменяя реквизиты документа, злоумышленник получает возможность управлять движением документа в системе, а соответственно изменять, получать и блокировать доступ, к информации, содержащейся в самом документе, и как следствие, к информации, содержащейся во всех процессах жизненного цикла документа[4,5].

Вероятность использования той или иной уязвимости, в свою очередь, определяется совокупностью следующих технических параметров системы:

1) Вид используемой в системе БД;

2) Способы аутентификации пользователей;

3) Открытость исходного кода;

4) Внутренняя архитектура взаимодействия модулей системы;

5) Наличие и способ реализации WEB-интерфейса;

6) Механизм подписания документа (включая виды используемых ЭП);

7) Наличие механизмов шифрования БД.

8) Протоколирование действий пользователя и системы, а также доступность данных протоколов.

Таким образом, согласно предложенной модели взаимосвязи уязвимостей и угроз безопасности информации в системах электронного документооборота можно установить, что одним из параметров, оказывающих наибольшее влияние на общий уровень защищенности системы электронного документооборота, являются уязвимости связанные с нарушением целостности реквизитов. Эффективными техническими мерами устранения данной угрозы является использование средств, направленных на контроль и управление доступом пользователей к ресурсам системы, а также использование электронной подписи позволяющей контролировать факт достоверности электронного документа.

Литература

1. ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения.

2. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».

3. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

4. ГОСТ Р ИСО/МЭК ТО 19791-2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.

5. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

References

1. GOST R 7.0.8-2013. Natsional'nyy standart Rossiyskoy Federatsii. Sistema standartov po informatsii, bibliotechnomu i izdatel'skomu delu. Deloproizvodstvo i arkhivnoye delo. Terminy i opredeleniya.

2. GOST R 53114-2008 Zashchita informatsii. Obespecheniye informatsionnoy bezopasnosti v organizatsii. Osnovnyye terminy i opredeleniya».

3. GOST R ISO/MEK 15408-2-2008 Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologiy. Chast' 2. Funktsional'nyye trebovaniya bezopasnosti.

4. GOST R ISO/MEK TO 19791-2008 Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Otsenka bezopasnosti avtomatizirovannykh sistem.

5. GOST R 51275-2006 Zashchita informatsii. Ob"yekt informatizatsii. Faktory, vozdeystvuyushchiye na informatsiyu. Obshchiye polozheniya

БАСЫРОВ Руслан Равильевич, аспирант кафедры «Информационные технологий и защита информации» Уральского государственного университета путей сообщения; 620034, г. Екатеринбург, ул. Колмогорова, 66, RRBasyirov@usurt.ru

ПАРШИН Константин Анатольевич, канд. тех. наук, доцент «Информационные технологий и защита информации» Уральского государственного университета путей сообщения; 620034, г. Екатеринбург, ул. Колмогорова, 66, KParshin@usurt.ru

BASYROV Ruslan Ravilevich, Postgraduate at the Department of «Information technologies and protection of information», Ural State University of Railway Transport, 620034, Ekaterinburg, Kolmogorov street, 66, RRBasyirov@usurt.ru

PARSHIN Konstantin Anatolevich, Candidate of Engineering Sciences, Associate Professor at the Department of «Information technologies and protection of information», Ural State University of Railway Transport, 620034, Ekaterinburg, Kolmogorov street, 66, KParshin@usurt.ru