www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.3.3

УДК 004.056.5
ББК 68.823

МОДЕЛЬ ВТОРЖЕНИЙ В ИНФОРМАЦИОННУЮ СИСТЕМУ

Дмитрий Владимирович Кленин

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
klenin-23@yandex.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Елена Александровна Максимова

Кандидат технический наук, доцент,
заведующая кафедрой информационной безопасности,
Волгоградский государственный университет
maksimova@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Определены категории «атака», «вторжение» и «инцидент» информационной безопасности. Выявлены виды вторжений в информационную систему и приведен их краткий анализ. Предложенная модель вторжений в информационную систему позволит практически на всех этапах жизненного цикла системы защиты информации повысить ее эффективность.

Ключевые слова: вторжение, информационная безопасность, информационная система, проектирование, модель.

В последнее время вопросы защиты информации стоят наиболее остро. Так, по данным компании InfoWatch, количество утечек конфиденциальной информации в первом полугодии 2018 г. на 12 % больше, чем за аналогичный период 2017 г., и равно 1 039 случаям [2]. При этом из 925 случаев утечки 73 % были реализованы при помощи вторжений в информационную систему.

Понятие вторжения тесно связано с понятиями «атака» и «инцидент» информационной безопасности (ИБ).

Под атакой понимают «действия, направленные на реализацию угроз несанкционированного доступа к информации, воздействия на нее или на ресурсы автоматизированный информационной системы с применением программных и (или) технических средств» [3]; «вредоносное воздействие, направленное на нарушение информационной безопасности и использующее уязвимости системы» [4]; «практическая реализация угрозы или попытка ее реализации с использованием той или иной уязвимости» [9]. Под инцидентом ИБ – «любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность» [3]; «появление одного или нескольких нежелательных, или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ» [4].

© Кленин Д.В., Максимова Е.А., 2018

Информационная система – это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [5].

Сложность нахождения проведенного вторжения и относительно легкая реализация последнего делает этот вид неправомерных действий очень опасным и усложняет процесс быстрого реагирования на атаку. Результатом такого воздействия является то, что у нарушителя появляется больше времени для атаки, вследствие чего у злоумышленника увеличиваются шансы успешной реализации задуманного [1].

Вторжения можно разделить по характеру воздействия на информационную систему. Они подразделяются на пассивные и активные. К *пассивным* можно отнести атаки, представляющие собой некоторое влияние, не оказывающее целенаправленного воздействия на работу системы, способное дезорганизовать ее политику безопасности. Отсутствие постоянного воздействия на функционирование информационной системы приводит именно к тому, что пассивное удаленное влияния трудно заметить. Одним из примеров такой атаки служит прослушивание канала связи в сети [8]. *Активное* воздействие на информационную систему – влияние, которое прямо воздействует на функционирование самой системы и подвергает опасности политику безопасности, принятую в ней. Активными влиянием являются почти все типы вторжений, которые происходят извне. Отличие активного влияния от пассивного – принципиальная возможность его выявления, так как в итоге его осуществления в системе случаются изменения, которые легко обнаружить. При пассивном же влиянии очень сложно обнаружить какие-либо следы воздействия на информационную систему [5].

Вторжения подразделяются по цели воздействия: нарушение работы системы (доступа к системе); нарушение целостности информационных ресурсов; нарушение конфиденциальности информационных ресурсов. Данная классификация соответствует трем основным видам вторжений – *отказ в обслуживании*, *раскрытие* и *нарушение целостности.*

Целью любого вторжения является получение несанкционированного доступа (НСД) к информации [8]. Существуют два способа получения информации: искажение и перехват. *Перехват* информации означает получение к ней доступа без возможности ее изменения. При перехвате информации появляется возможность ее копировать, что является примером нарушения конфиденциальности информации. В таком случае имеется неправомерный доступ, но отсутствуют варианты подмены информации. Нарушение конфиденциальности относиться к пассивным воздействиям [7].

Фальсификацию (искажение, подмену) информации можно классифицировать как полный контроль над потоками информации между объектами или передачу сообщений от пользователя системы, которая была взломана. Подмена информации приводит к нарушению целостности и является примером активного воздействия на информационную систему. Ложный объект информационной системы является примером вторжения для нарушения целостности информации.

Вторжения классифицируют по наличию связи с атакуемым объектом. Их подразделяют на два класса: с обратной связью и без обратной связи [8]. Если атака осуществляется *с обратной связью*, то злоумышленник отправляет некоторые пакеты на атакуемый объект, на которые ожидает получить ответ. Из-за этого между хакером и машиной, которая должна быть взломана, появляется обратная связь, позволяющая злоумышленнику реагировать на все перемены на атакуемом объекте. В случае, когда атака осуществляется *без обратной связи*, злоумышленнику нет необходимости реагировать на изменения на атакуемой машине. Эти вторжения реализуются при помощи передачи на атакуемый объект одиночных запросов. Злоумышленник не ждет ответы на эти запросы [6].

Вторжения делятся на вторжения по запросу от атакуемого объекта, вторжения по наступлении ожидаемого события на атакуемом объекте и безусловное.

При вторжении *по запросу от атакуемого объекта* действие со стороны злоумышленника осуществляется при условии, что атакуемая машина отправит запрос определенного типа.

При вторжении *по наступлении ожидаемого события на атакуемом объекте*

злоумышленник постоянно проводит мониторинг состояния операционной системы удаленной машины и начинает действие при возникновении конкретного события в этой системе.

Безусловное вторжение осуществляется сразу после того, как атакующий выбрал цель и независимо от состояния операционной системы и атакуемого объекта предпринимает атаку.

По расположению субъекта вторжения относительно атакуемого объекта подразделяют на *межсегментное* и *внутрисегментное* вторжение.

Модель вторжений в ИС представлена на рисунке.

Знание исследованных классов вторжений наиболее эффективно на этапе проектирования системы защиты информации [7; 8]. Кроме того, использование данной модели при расследовании инцидентов ИБ позволит повысить эффективность работы и снизить риски ИБ [6].

Использование предложенной модели связано с решением конкретных практических задач в области информационной безопасности, в том числе с определением уязвимостей ИС. Последнее, в свою очередь, необходимо для определения элементов системы защиты. Например, на стадии проектирования СЗИ при выборе программных средств защиты нужно учитывать расположение субъекта вторжения относительно атакуемого объекта.

При работе с функционирующей на предприятии СЗИ, то есть при решении вопросов ее модернизации или оптимизации, вопросы внесения изменений в состав СЗИ решаются в соответствии: 1) со статистическими данными по вторжениям в ИС; 2) с имеющимися результатами инцидентов информационной безопасности; 3) с прогнозными данными.

Таким образом, предложенная модель вторжений в ИС является одним из внешних условий при работе с системой защиты информационной системы организации (предприятия) и вполне может определять (задавать) уровень риска информационной безопасности предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Герасименко, В. А. Основы защиты информации / В. А. Герасименко, А. А. Малюк. – М. : МИФИ, 1997. – 537 с.

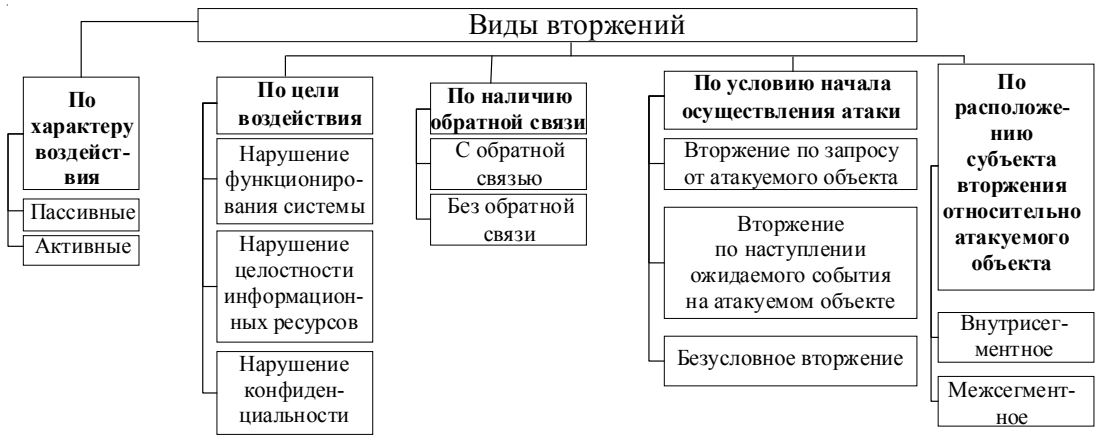
2. Глобальное исследование утечек конфиденциальной информации в 1 полугодии 2018 года // Infowatch : [сайт]. – Электрон. дан. – Режим доступа: https://www.infowatch.ru/report2018_half (дата обращения: 04.10.2017). – Загл. с экрана.

3. ГОСТ Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации : введ. 2006-02-01. – М. : Стандартинформ, 2006. – 15 с.

4. ГОСТ Р ИСО/МЭК 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности : введ. 2008-07-01. – М. : Стандартинформ, 2009. – 50 с.

5. Избачков, Ю. С. Информационные системы / Ю. С. Избачков. – М. : Информ, 2006. – 378 с.

6. Максимова, Е. А. Архитектура программного комплекса предотвращения инсайдерской активности и оценки эффективности работы персонала организации / Е. А. Максимова, Е. А. Витенбург // Информационные системы и технологии :



Модель вторжений в информационную систему

научно-технический журнал. Рубрика «Информационная безопасность». – 2016. – № 2.

7. Максимова, Е. А. Формализация процесса обеспечения информационной безопасности при реализации инсайдерских атак / Е. А. Максимова, Е. А. Витенбург // Известия ТулГУ. Технические науки. – 2015. – Вып. 8, ч. 2. – С. 231–238.

8. Максимова, Е. А. Цепи Маркова как средство прогнозирования инсайдерских вторжений / Е. А. Максимова, Е. А. Витенбург, В. А. Корнева // Проблемы информационной безопасности. Компьютерные системы. – 2015. – № 4. – С. 9–12.

9.Система обнаружения вторжений. – Электрон. дан. – Режим доступа: https://ru.wikipedia.org /wiki/Система_обнаружения_вторжений (дата обращения: 0 2.10.2017). – Загл. с экрана.

REFERENCES

1. Gerasimenko V.A., Malyuk A.A. *Osnovy zashchity informatsii* [Basics of Information Security]. Moscow, MIFI Publ., 1997. 537 p.

2. Globalnoe issledovanie utechek konfidentsialnoy informatsii v 1 polugodii 2018 goda [Global Research of Confidential Information Leaks in the First Half of 2018]. *Infowatch: website*. URL: https:/ /www.infowatch.ru/report2018_half (accessed 4 October 2017).

3. *GOST R 50.1.053-2005. Informatsionnye tekhnologii. Osnovnye terminy i opredeleniya v oblasti tekhnicheskoy zashchity informatsi: vved. 2006-02-01* [GOST R 50.1.053-2005. Information Technology. The Basic Terms and Definitions in the Field of Technical Protection of Information: Introduced on 1 February 2006]. Moscow, Standartinform Publ., 2006. 15 p.

4. *GOST R ISO/MEK 18044-2007. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment intsidentov informatsionnoy bezopasnosti: vved. 2008-07-01* [GOST R ISO/MEK 18044-2007. Information Technology. Methods and Means of Security. Information Security Incident Management: Introduced on 1 July 2008]. Moscow, Standartinform Publ., 2009. 50 p.

5. Izbachkov Yu.S. *Informatsionnye sistemy* [Information Systems]. Moscow, Inform Publ., 2006. 378 p.

6. Maksimova E.A., Vitenburg E.A. Arkhitektura programmnogo kompleksa predotvrashcheniya insayderskoy aktivnosti i otsenki effektivnosti raboty personala organizatsii [Architecture of the Software Package for Preventing Insider Activity and Evaluating the Performance of the Company's Staff]. *Informatsionnye sistemy i tekhnologii: nauchno-tekhnicheskiy zhurnal. Rubrika «Informatsionnaya bezopasnost»*, 2016, no. 2.

7. Maksimova E.A., Vitenburg E.A. Formalizatsiya protsessa obespecheniya informatsionnoy bezopasnosti pri realizatsii insayderskikh atak [Formalization of the Process of Ensuring Information Security in the Implementation of Insider Attacks]. *Izvestiya TulGU. Tekhnicheskie nauki*, 2015, iss. 8, part 2, pp. 231-238.

8. Maksimova E.A., Vitenburg E.A., Korneva V.A. Tsepi Markova kak sredstvo prognozirovaniya insayderskikh vtorzheniy [Markov's Chains as a Means of Predicting Insider Intrusions]. *Problemy informatsionnoy bezopasnosti. Kompyuternye sistemy*, 2015, no. 4, pp. 9-12.

9. *Sistema obnaruzheniya vtorzheniy* [Intrusion Detection System]. URL: https://ru.wikipedia.org/wiki/ Sistema_obnaruzheniya_vtorzheniy (accessed 2 October 2017).

THE MODEL OF INTRUSION INTO THE INFORMATION SYSTEM

Dmitriy V. Klenin

Student, Department of Information Security,
Volgograd State University
klenin-23@yandex.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Elena A. Maksimova

Candidate of Sciences (Engineering), Associate Professor, Head of Department of Information Security,
Volgograd State University
maksimova@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. Categories ‘attack’, ‘intrusion’ and ‘incident’ of information security are defined. The types of intrusions into the information system are revealed, and their brief analysis is given. The proposed model of intrusion into the information system will allow to increase its efficiency at almost all stages of the information security system life cycle.

The use of the proposed model is associated with the solution of specific practical problems in the field of information security, including the definition of vulnerabilities of the information system. The latter, in turn, is necessary to determine the elements of the protection system. For example, at the design stage of the information security system, when choosing software protection you need to take into account the location of the intruder relative to the attacked object.

When working with functioning systems of information protection, i.e. at the solution of questions of modernization or optimization, changes in the system of information security are resolved in accordance with statistical data for the intrusion into the information system with available results of information security incidents, with the forecast data.

Thus, the proposed model of intrusion into the information system is one of the external conditions when working with the information system of the organization (enterprise) may well determine (set) the level of risk of information security of the enterprise.

Key words: intrusion, information security, information system, design, model.