

УДК 004.056

## **КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ**

*Исмоилов З.Ш., студент 3 курса экономического факультета  
Научный руководитель – Климущкина Н.Е., кандидат  
экономических наук, доцент  
ФГБОУ ВО Ульяновский ГАУ*

**Ключевые слова:** *информационные системы, угрозы, информационная безопасность.*

*Угроза «информационной безопасности» – это потенциальная возможность нарушения режима информационной безопасности, которая прямо или косвенно может нанести урон пользователю. В статье рассматриваются наиболее распространенные угрозы безопасности в информационных системах.*

Информационные системы часто подвергаются различным типам угроз, которые могут вызвать повреждения, приводящие впоследствии к значительным финансовым потерям. Ущерб информационной безопасности может варьироваться от небольших потерь до полного разрушения информационной системы [1]. Влияние различных угроз значительно различается: одни влияют на конфиденциальность или целостность данных, а другие влияют на доступность системы. В настоящее время организации пытаются понять, что представляют собой угрозы для их информационных активов и как получить необходимые средства для борьбы с ними, что по-прежнему представляет собой проблему [2].

При изучении вопросов угрозы безопасности в информационных системах, сначала необходимо рассмотреть такие понятия, как источник, агент, мотивация и намерение.

Источник угрозы безопасности - угроза может быть вызвано как внутренними, так и внешними субъектами. Внутренние угрозы возникают, когда кто-то имеет авторизованный доступ к сети с учетной записью. Внешние, впоследствии атаки за пределами организации.

Агенты угроз – это субъект, который навязывает угрозу системе. Было выделено три класса для нашей конкретной классификации: люди, стихийные бедствия и технологические угрозы.

Мотивация угрозы – злоумышленники обычно имеют конкретную цель или мотив для атаки на систему. Эти цели могут привести к вредоносным или не вредоносным результатам.

Намерение угрозы –

- Преднамеренные угрозы представляют собой угрозы, которые являются результатом вредоносного решения. Например, компьютерные преступления, или когда кто-то намеренно повреждает имущество или информацию.
- Непреднамеренные угрозы представляют собой угрозы, которые вводятся без ведома. Эти угрозы в основном включают несанкционированное или случайное изменение программного обеспечения [3].

Угрозы исходят из разных источников, таких как действия сотрудников или хакерские атаки. Уязвимости состоят из слабых мест в системе, которые могут быть использованы злоумышленниками, что может привести к опасным последствиям. Согласно 11-му ежегодному исследованию компьютерной преступности и безопасности, 74,3% всех потерь вызваны: вирусами, несанкционированным доступом, кражей портативного или мобильного оборудования и кражи конфиденциальной информации (рисунок 1) [2].

Чтобы обезвредить эти угрозы, необходимо знать источники угроз и конкретные области системы, которые могут быть затронуты [4].

Основными источниками угроз являются отдельные злоумышленники («хакеры»), киберпреступные группы и т.д. Чтобы пробиться



**Рисунок 1 – Угрозы информационной безопасности**

через защиту и получить доступ к нужной информации, они используют слабые места и ошибки в работе программного обеспечения и веб-приложений, изъяны в конфигурациях сетевых экранов и настройках прав доступа, прибегают к прослушиванию каналов связи и использованию клавиатурных шпионов [4].

Информационная безопасность является критической проблемой для отдельных лиц и организаций, поскольку она приводит к большим финансовым потерям. На сегодняшней день задачей России в сфере информационной безопасности являются только часть общемировых задач и проблем. Общее соотношение угроз в мире показывает, что Россия находится на втором месте по количеству кибертеррористических актов и хакерских атак. Однако если в США совершается 41% всех хакерских атак в мире, в России – не более 10%. Сложившаяся ситуация дает возможность воспользоваться относительно комфортным режимом и направить силы на повышение уровня защиты от предполагаемых угроз.

#### *Библиографический список:*

1. Influence of the exchange of cybersecurity information when investing / L. A. Gordon, M. P. Loeb, V. Luchishin, L. Zhou // *Prospective real options*. - 2016. - № 34. – PP. 509-519.
2. Классификация угроз информационной безопасности. – URL : <https://studfile.net/preview/4518611/page:3/>
3. Информационная безопасность бизнеса Результаты исследования. Лаборатория «Касперского». - URL : [http://media.kaspersky.com/pdf/IT\\_risk\\_report\\_Russia\\_2012.pdf](http://media.kaspersky.com/pdf/IT_risk_report_Russia_2012.pdf)
4. Международное исследование ЕУ в области информационной безопасности «Путь к киберустойчивости: прогноз, сопротивление, ответная реакция». – URL : <https://www.anti-malware.ru/threats/information-security-threats>
5. Хамзина, О. И. Учетно-аналитическое обеспечение экономической безопасности предприятия / О. И. Хамзина, Е. В. Банникова // *Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения, посвященной 75-летию Ульяновского государственного аграрного университета им. П.А. Столыпина* : материалы IX Международной научно-практической конференции. – Ульяновск : УлГАУ, 2018. - С. 369-374.
6. Хамзина, О. И. Роль риск-менеджмента в обеспечении экономической безопасности сельскохозяйственного предприятия / О. И. Хамзина, И. И. Хамзин, Е. В. Банникова // *Экономика и предпринимательство*. - 2018. - № 11 (100). - С. 1136-1139.

7. Банникова, Е. В. Внутренний аудит в системе экономической безопасности / Е. В. Банникова, О. И. Хамзина, А. А. Навасардян // Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения : материалы Национальной научно-практической конференции. – Ульяновск : УлГАУ, 2019. - С. 225-229.
8. Навасардян, А. А. Анализ эколого-экономической безопасности Ульяновской области и мероприятия по ее обеспечению / А. А. Навасардян, О. И. Хамзина, Е. В. Банникова // Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения : материалы Национальной научно-практической конференции. – Ульяновск : УлГАУ, 2019. - С. 299-304.

## CLASSIFICATION OF SECURITY THREATS IN INFORMATION SYSTEMS

*Ismailov Z.*

**Keywords:** *information systems, threats, information security.*

*The threat to “information security” is a potential possibility of violating the information security regime, which can directly or indirectly cause damage to the user. The article discusses the most common security threats in information systems.*