Столыпинский вестник

Научная статья
Original article
УДК 004.056

# ПРИМЕНЕНИЕ МОДЕЛИ ОЦЕНКИ ДОВЕРИЯ НА ОСНОВЕ СУБЪЕКТИВНОЙ ЛОГИКИ К СОБЫТИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КИБЕРИГРАХ

# APPLICATION OF A TRUST ASSESSMENT MODEL BASED ON SUBJECTIVE LOGIC TO INFORMATION SECURITY EVENTS IN CYBER GAMES

**Киров А.Д.,** аспирант 3 курс, кафедра Прикладной информатики и информационной безопасности, РЭУ им. Г.В. Плеханова,
Россия, г. Москва kirow.alesha@yandex.ru

**Kirov A.D.,** PhD student 3rd year, Department of Applied Informatics and Information Security, Plekhanov Russian University of Economics

**Аннотация:** Статья посвящена применению модели оценки доверия к событиям информационной безопасности (ИБ). На основе анализа модели субъективной логики, предназначенной для определения уровней доверия субъектов к объектам, разработана модель оценки доверия к событиям ИБ, позволяющая определять уровень доверия событиям и инцидентам ИБ. В отличие от существующих моделей оценки уровня доверия к объектам ИБ, предложенная модель позволяет учесть субъективность убеждений лиц, оценивающих уровни доверия к событиям и инцидентам ИБ. Разработанная

модель позволяет определять уровень доверия к автоматически или автоматизировано-выявленным инцидентам ИБ для повышения эффективности анализа событий и инцидентов ИБ. Оценено применение разработанной модели в кибериграх.

**Abstract:** The article is devoted to the application of a model for assessing trust in information security (IS) events. Based on the analysis of a model of subjective logic designed to determine the levels of trust of subjects to objects, a model for assessing trust in information security events has been developed, which allows determining the level of trust in information security events and incidents. Unlike existing models for assessing the level of trust in information security facilities, the proposed model allows us to take into account the subjectivity of the beliefs of persons assessing the levels of trust in information security events and incidents. The developed model allows us to determine the level of trust in automatically or automatically identified information security incidents in order to increase the effectiveness of the analysis of information security events and incidents. The application of the developed model in cyber games is evaluated.

**Ключевые слова:** доверие; субъективная логика; событие информационной безопасности; инцидент информационной безопасности; модель оценки; эксперт.

**Keywords:** confidence; subjective logic; information security event; information security incident; assessment model; expert.

В настоящее время в связи с повышением уровня угроз информационной безопасности (ИБ) и активизацией действий нарушителей ИБ, задачи мониторинга ИБ приобретают особую актуальность [1-2]. Большинство систем мониторинга ИБ представляют собой автоматизированные системы, работающие с событиями ИБ, обеспечивая процессы их сбора, нормализации (приведения к единообразному виду), централизованного анализа и выявления инцидентов ИБ [3-6]. Задачи выявления инцидентов ИБ в таких системах решаются автоматизированным образом при помощи системы правил,

определяющих, является ли событие ИБ инцидентом ИБ, или входит в его состав, или нет. Такие правила составляются экспертами в области выявления инцидентов ИБ [7]. Также для выявления инцидентов ИБ применяются методы искусственного интеллекта, позволяющие систем мониторинга ИБ автоматически определять вероятность того, является ли событие ИБ инцидентом ИБ, или входит в его состав, или нет [8]. Так как система правил строится на основе убеждений экспертов в области выявления инцидентов ИБ, а модули автоматического выявления инцидентов ИБ используют методы искусственного интеллекта, становится актуальной задача оценки доверия к событиям информационной безопасности.

**Цель исследования**

В настоящее время задачи оценки доверия к событиям ИБ решаются индивидуально для каждого конкретного случая. В процессе мониторинга ИБ специалист в области ИБ самостоятельно оценивает вероятность того, является ли событие ИБ инцидентом ИБ, или нет, с использованием всех имеющихся у него данных и опыта [9]. Однако, система правил, позволяющая автоматизированным способом выявлять инциденты ИБ, опирается на использование уже имеющихся знаний и опыта специалиста в области ИБ компании (в случае, если правила, выявляющие инциденты ИБ, были написаны им), либо другими экспертами в области выявления инцидентов ИБ (в случае, если правила, выявляющие инциденты ИБ, были получены из сторонних источников) [10]. Так как в настоящее время выявление инцидентов ИБ зачастую проводится на основе правил SIEM-систем в автоматизированном режиме, либо эмпирическим способом, становится актуальной задача определения уровней доверия к событиям ИБ как к исходным данным, на основе которых принимаются решения относительно того, является ли событие ИБ инцидентом ИБ, или нет, так и к системам таких правил. В связи с вышеизложенным, эта задача может быть сформулирована в виде оценки доверия к событиям ИБ конкретных экспертов в области выявления инцидентов ИБ, так как она объединяет в себе как доверие к исходным данным в виде событий ИБ, так и

доверие к убеждениям экспертов относительно того, является ли конкретное событие ИБ инцидентом ИБ, или нет, в виде правил, непосредственно отвечающим за выявление инцидентов ИБ.

**Основная часть**

Для решения задачи оценки доверия к событиям ИБ целесообразно использовать модель субъективной логики [11], позволяющую учитывать субъективность убеждений лиц, оценивающих уровни доверия к событиям и инцидентам ИБ.

При применении модели субъективной логики [11] к оценке уровня доверия к событиям ИБ и инцидентам ИБ, её параметры могут быть интерпретированы следующим образом:

$b_x$ – убеждённость эксперта в области выявления инцидентов ИБ в том, что событие ИБ является инцидентом ИБ, либо входит в его состав;

$d_x$ – убеждённость эксперта в области выявления инцидентов ИБ в том, что событие ИБ не является инцидентом ИБ, либо не входит в его состав;

$u_x$ – убеждённость эксперта в области выявления инцидентов ИБ в том, что из данных события ИБ невозможно сделать вывод о том, является оно инцидентом ИБ, или нет;

$a_x$ – априорная вероятность того, что событие ИБ является инцидентом ИБ, либо входит в его состав, определённая модулем искусственного интеллекта, включаемого в состав некоторых систем мониторинга ИБ (в случае его отсутствия $a_x = 0$).

Оценка уровня доверия к событиям ИБ и инцидентам ИБ с использованием модели субъективной логики осуществляется следующим образом:

1. Если параметр $u_x$ эксперта по отношению к событию ИБ $\geq 0,5$, то для определения того, является оно инцидентом ИБ, или нет, используется параметр $a_x$ (если параметр $a_x \geq 0,5$, то событие ИБ является инцидентом ИБ, нет в противном случае);

2. Если параметр $u_x$ эксперта по отношению к событию ИБ <0,5, то для определения того, является оно инцидентом ИБ, или нет, используются параметры $b_x$ и $d_x$ (если параметр $b_x \geq d_x$, то событие ИБ является инцидентом ИБ, нет в противном случае).

Уровень доверия к убеждению любого эксперта по отношению к любому событию ИБ должен оцениваться с учётом особенностей используемой модели, а именно, её чувствительности к исходным данным. В случае использования модели субъективной логики, он может быть оценён по формуле [12]:

$$L_{tr} = \sqrt{(b_x)^2 + (d_x)^2}, \quad (1.1)$$

где $L_{tr}$ - уровень доверия к убеждению эксперта в области выявления инцидентов ИБ;

$b_x$ – убеждённость эксперта в области выявления инцидентов ИБ в том, что событие ИБ является инцидентом ИБ, либо входит в его состав;

$d_x$ – убеждённость эксперта в области выявления инцидентов ИБ в том, что событие ИБ не является инцидентом ИБ, либо не входит в его состав.

Если уровень доверия к убеждению эксперта по отношению к событию ИБ $\geq 0,5$, то доверие эксперту может быть оказано, иначе доверие эксперту не может быть оказано.

Если доверие убеждениям всех экспертов по отношению к событию ИБ не может быть оказано, для определения того, является оно инцидентом ИБ, или нет, используется параметр $a_x$ (если параметр $a_x \geq 0,5$, то событие ИБ является инцидентом ИБ, нет в противном случае).

**Полученные результаты**

Оценка эффективности применения модели оценки доверия к событиям информационной безопасности выполнена на примере киберигры, проведённой среди студентов ФГБОУ ВО «РЭУ им. Г.В. Плеханова» направления 10.03.01 «Информационная безопасность» 29.12.2023. Цель киберигры – развитие у

студентов практических навыков информационного противоборства в киберпространстве.

При проведении киберигры группа студентов псевдослучайным образом разделена на 2 команды – «Атакующих» («Red Team») и «Защитников» («Blue Team»), имеющих разные цели.

Цель атакующих – получить контроль над инфраструктурой, включающей уязвимый домен Active Directory и уязвимые рабочие станции, проэксплуатировав уязвимости в ней с использованием рабочих станций для компрометации уязвимого домена и уязвимых рабочих станций.

Цель защитников – обнаружить действия атакующих, осуществив мониторинг событий информационной безопасности и выявление инцидентов информационной безопасности с использованием системы мониторинга событий информационной безопасности и соответствующим образом обработав выявленные инциденты информационной безопасности с использованием межсетевого экрана с модулем обнаружения и предотвращения вторжений и системы мониторинга событий информационной безопасности.

Для проведения киберигры группе студентов, принимающей в них участие, предоставлен набор материально-технического обеспечения, включающий следующие компоненты:

- уязвимый домен Active Directory на базе Windows Server 2012;
- уязвимые рабочие станции на базе Windows 8 (5 шт.);
- межсетевой экран с модулем обнаружения и предотвращения вторжений на базе Ideco UTM;
- система мониторинга событий информационной безопасности на базе Komrad SIEM;
- рабочие станции для компрометации уязвимого домена и уязвимых рабочих станций (5 шт.) с инструментами: Kali Linux, Nmap, OpenVAS, Metasploit Framework, BEEF Framework;
- выборка из матрицы техник и тактик нарушителей кибербезопасности MITRE ATTACK [13].

Обобщенный сценарий действий команды атакующих может включать следующие шаги:

1. Изучение выборки из матрицы техник и тактик нарушителей кибербезопасности MITRE ATTACK;
2. Изучение предоставленной уязвимой инфраструктуры на предмет наличия в ней известных уязвимостей;
3. Выбор из выборки матрицы техник и тактик нарушителей кибербезопасности MITRE ATTACK тактик и техник, предполагающих эксплуатацию выявленных уязвимостей;
4. Расположение выбранных техник и тактик так, чтобы они могли быть выполнены последовательно и их последовательное выполнение приводило к компрометации предоставленной уязвимой инфраструктуры, представление их в виде сценария нарушителя кибербезопасности;
5. Реализация построенного сценария нарушителя кибербезопасности, путём осуществления эксплуатации выявленных уязвимостей с использованием предоставленных инструментов.

Обобщенный сценарий действий команды защитников может включать следующие шаги:

1. Изучение предоставленных инструментов ИБ (межсетевого экрана с модулем обнаружения и предотвращения вторжений на базе Ideco UTM и системы мониторинга событий информационной безопасности на базе Komrad SIEM) с использованием руководств пользователя и администратора;
2. Изучение предоставленной уязвимой инфраструктуры на предмет наличия в ней известных уязвимостей;
3. Изучение выборки из матрицы техник и тактик нарушителей кибербезопасности MITRE ATTACK на предмет возможных используемых нарушителями кибербезопасности техник и тактик;
4. Выявление инцидентов ИБ;
5. В случае успешного выявления инцидентов ИБ, их обработка.

События информационной безопасности, сгенерированные в процессе проведения киберигры приведены в таблице 1.

Таблица 1.

События информационной безопасности, сгенерированные в процессе проведения киберигры

| **№ п\п** | **Наименование события ИБ** | **Является инцидентом ИБ, или входит в его состав при оценке участниками киберигры** |
|---|---|---|
| 1 | Неправильный ввод пароля на рабочей станции, работающей на базе ОС Windows 8 | Нет |
| 2 | Неправильный ввод пароля на контроллере домена, работающего на базе ОС Windows Server 2012R2 | Да |
| 3 | Неправильный ввод пароля на рабочей станции, работающей на базе ОС Kali Linux 2023.1 | Нет |
| 4 | Успешный вход на рабочую станцию, работающую на базе ОС Windows 8 с именем пользователя, входящего в группу локальных администраторов | Нет |
| 5 | Успешный вход на рабочую станцию, работающую на базе ОС Windows 8 с именем пользователя, входящего в группу администраторов домена | Нет |
| 6 | Успешный вход на рабочую станцию, работающую на базе ОС Windows 8 с именем пользователя, входящего в группу системных пользователей | Да |
| 7 | Успешный вход на контроллер домена, работающего на базе ОС Windows Server 2012R2, входящего в группу администраторов домена | Нет |
| 8 | Успешный вход на контроллер домена, работающего на базе ОС Windows Server 2012R2, входящего в группу системных пользователей | Да |
| 9 | Сетевая атака | Да |

Вышеуказанные события ИБ были оценены 2 экспертами в области выявления инцидентов ИБ, являющимися участниками киберигры, показавшими лучшие результаты. Полученные параметры оценок событий ИБ приведены в таблице 2.

Таблица 2.

Параметры оценок событий информационной безопасности, сгенерированных в процессе проведения киберигры 2 экспертами в области выявления инцидентов ИБ

| № п\п | Наименование события ИБ | № эксперта в области выявления инцидентов ИБ | Значение $b_x$ | Значение $d_x$ | Значение $u_x$ | Значение $a_x$ | Является инцидентом ИБ, или входит в его состав при оценке экспертом | Уровень доверия к эксперту в области выявления инцидентов ИБ | Доверие к эксперту в области выявления инцидентов ИБ | Является инцидентом ИБ, или входит в его состав |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Неправильный ввод пароля на рабочей станции, работающей на базе ОС Windows 8 | 1 | 0,3 | 0,6 | 0,1 | 0,2 | Нет | 0,67 | Оказано | Нет |
| | | 2 | 0,6 | 0,35 | 0,05 | | Да | 0,69 | Оказано | Да |
| 2 | Неправильный ввод пароля на контроллере домена, работающего на базе ОС Windows Server 2012R2 | 1 | 0,65 | 0,3 | 0,05 | 0,8 | Да | 0,72 | Оказано | Да |
| | | 2 | 0,3 | 0,65 | 0,05 | | Нет | 0,72 | Оказано | Нет |
| 3 | Неправильный ввод пароля на рабочей станции, работающей на базе ОС Kali Linux 2023.1 | 1 | 0,2 | 0,2 | 0,6 | 0,55 | Да | 0,28 | Не оказано | Да |
| | | 2 | 0,3 | 0,15 | 0,55 | | Да | 0,34 | Не оказано | Да |
| 4 | Успешный вход на рабочую станцию, работающую на базе ОС Windows 8 с именем пользователя, входящего в группу локальных администраторов | 1 | 0,8 | 0,1 | 0,1 | 0,2 | Да | 0,81 | Оказано | Да |
| | | 2 | 0,75 | 0,2 | 0,05 | | Да | 0,78 | Оказано | Да |
| 5 | Успешный вход на рабочую станцию, работающую на базе ОС Windows 8 с именем пользователя, входящего в группу администраторов домена | 1 | 0,4 | 0,05 | 0,55 | 0,8 | Нет | 0,4 | Не оказано | Да |
| | | 2 | 0,5 | 0,2 | 0,3 | | Да | 0,54 | Оказано | Да |

| № п\п | Наименование события ИБ | № эксперта в области выявления инцидентов ИБ | Значение $b_x$ | Значение $d_x$ | Значение $u_x$ | Значение $a_x$ | Является инцидентом ИБ, или входит в его состав при оценке экспертом | Уровень доверия к эксперту в области выявления инцидентов ИБ | Доверие к эксперту в области выявления инцидентов ИБ | Является инцидентом ИБ, или входит в его состав |
|---|---|---|---|---|---|---|---|---|---|---|
| 6 | Успешный вход на рабочую станцию, работающую на базе ОС Windows 8 с именем пользователя, входящего в группу системных пользователей | 1 | 0,6 | 0,4 | 0 | 0,8 | Да | 0,72 | Оказано | Да |
| | | 2 | 0,7 | 0,2 | 0,1 | | Да | 0,73 | Оказано | Да |
| 7 | Успешный вход на контроллер домена, работающего на базе ОС Windows Server 2012R2, входящего в группу администраторов домена | 1 | 0,2 | 0,65 | 0,15 | 0,45 | Нет | 0,68 | Оказано | Нет |
| | | 2 | 0,15 | 0,7 | 0,15 | | Нет | 0,72 | Оказано | Нет |
| 8 | Успешный вход на контроллер домена, работающего на базе ОС Windows Server 2012R2, входящего в группу системных пользователей | 1 | 0,8 | 0,2 | 0 | 0,9 | Да | 0,82 | Оказано | Да |
| | | 2 | 0,95 | 0,05 | 0 | | Да | 0,95 | Оказано | Да |
| 9 | Сетевая атака | 1 | 0,5 | 0,5 | 0 | 0,5 | Да | 0,7 | Оказано | Да |
| | | 2 | 0,5 | 0 | 0,5 | | Да | 0,5 | Оказано | Да |

Анализ данных таблиц 1-2 показал, что события ИБ № 3, 4 и 5 не были классифицированы как инциденты ИБ при их оценке участниками киберигры, но при их оценке экспертами в области выявления инцидентов ИБ, их принадлежность к категории инцидентов ИБ стала более явной. Использование модели оценки доверия к событиям ИБ в ряде случаев может позволить участникам киберигры, входящим в команду защитников, более эффективно выявлять инциденты ИБ, что может повысить их шансы на победу в киберигре.

**Заключение**

Применение моделей оценки доверия к событиям ИБ позволяет комплексно учесть субъективность убеждений лиц, оценивающих уровни доверия к событиям и инцидентам ИБ. Это позволяет в ряде случаев более эффективно выявлять инциденты ИБ, что может повысить шансы на победу команды защитников, выявляющих и обрабатывающих инциденты ИБ, в киберигре.

**Использованные источники:**

1. Сизов В.А. Проблемы внедрения SIEM-систем в практику управления информационной безопасностью субъектов экономической деятельности / В.А. Сизов, А.Д. Киров // Открытое образование. – 2020. – Т. 2, № 1. – С. 69-79 https://doi.org/10.21686/1818-4243-2020-1-69-79
2. Kirov, A. Development of a method for targeted monitoring and processing of information security incidents of economic entities. / Kirov, A., Sizov, V. // J Comput Virol Hack Tech. – 2022. – pp. 1-6 –https://doi.org/10.1007/s11416-022-00449-8
3. Kotenko, Igor. Model of security in-formation and event management system. / Kotenko, Igor & Parashchuk, Igor // Vestnik of Astrakhan State Technical University. Series: Management, computer science and informatics. 2020. – P. 84-94. – 10.24143/2072-9502-2020-2-84-94.
4. Ерышов, В. Г. Модель процесса мониторинга информационной безопасности в информационно-телекоммуникационных системах на основе применения аппарата теории марковских случайных процессов / В.

Г. Ерышов, Д. В. Ильина // Волновая электроника и инфокоммуникационные системы: Сборник статей XXIII международной научной конференции, Санкт-Петербург, 01–05 июня 2020 года. – Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2020. – С. 236-242. – EDN BDOQWB.

5. Королев, В. И. Процессная модель мониторинга и реагирования на инциденты информационной безопасности / В. И. Королев // Информационная безопасность: вчера, сегодня, завтра: Сборник статей по материалам III Международной научно-практической конференции, Москва, 23 апреля 2020 года. – Москва: Российский государственный гуманитарный университет, 2020. – С. 18-25. – EDN APZTCW.
6. Сизов В.А. Разработка моделей аналитической системы обработки данных для мониторинга ИБ объекта информатизации, использующего облачную инфраструктуру / В.А. Сизов, А.Д. Киров // Российский технологический журнал. – 2021. – С. 16-25.
7. Какие техники MITRE ATT&CK выявляют продукты Positive Technologies. – URL: https://mitre.ptsecurity.com/ru-RU/techniques?utm_source=seclab&utm_medium=news (дата обращения: 1.03.2024)
8. Onyango, Oscar. Artificial Intelligence and its Application to Information Security Management / Onyango, Oscar. 10.13140/RG.2.2.12066.09921.
9. Сидорова, Д. Н. Алгоритмы и методы кластеризации данных в анализе журналов событий информационной безопасности / Д. Н. Сидорова, Е. Н. Пивкин // Безопасность цифровых технологий. – 2022. – № 1(104). – С. 41-60. – DOI 10.17212/2782-2230-2022-1-41-60. – EDN RMDHEC.
10. PT Expert Security Center. – URL: https://www.ptsecurity.com/ru-ru/services/esc/ (дата обращения: 1.03.2024)
11. Jøsang A. Subjective Logic. A Formalism for Reasoning Under Uncertainty. – Springer International Publishing, Switzerland, 2016. – 337 p. ISBN 978-3-319-42335-7(1). DOI 10.1007/ 978-3319-42337-1.

12. Park Y. On the optimality of trust network analysis with subjective logic. Advances in Electrical and Computer Engineering, 14(3):49–54, 2014.
13. MITRE ATT&CK. – URL: https://attack.mitre.org/ (дата обращения: 1.03.2024)

**The sources used:**

1. Sizov V.A. Problems of implementing a SIEM system in the practice of intellectual property management / V.A. Sizov. Syzov, A.D. Kirov // Open education. - 2020. – vol. 2, No. 1. – pp. 69-79 https://doi.org/10.21686/1818-4243-2020-1-69-79
2. Kirov, A. Development of a method for targeted monitoring and processing of information security incidents of economic entities / A. Kirov. / Kirov A., Sizov V. // Computer hacking technology. – 2022. – pp. 1-6 – https://doi.org/10.1007/s11416-022-00449-8
3. Kotenko, Igor. A model of a security information and event management system. Kotenko, Igor and Paraschuk, Igor // Bulletin of the Astrakhan State Technical University. Series: Management, Computer Science and Computer Science. 2020. – pp. 84-94. – 10.24143/2072-9502-2020-2-84-94.
4. Yeryshov, V. G. Model of the process of monitoring information security in information and telecommunication systems based on the application of the apparatus of the theory of Markov random processes / V. G. Yeryshov, D. V. Ilyina // Wave electronics and infocommunication systems: Collection of articles of the XXIII international scientific conference, St. Petersburg, June 01-05, 2020. – St. Petersburg: St. Petersburg State University of Aerospace Instrumentation, 2020. – pp. 236-242. – ED. BDOQWB.
5. Korolev, V. I. Process model of monitoring and responding to information security incidents / V. I. Korolev // Information security: yesterday, today, tomorrow: Collection of articles based on the materials of the III Scientific and Practical International Conference, Moscow, April 23, 2020. – Moscow: Russian State University for the Humanities, 2020. – pp. 18-25. – PUBLISHING house APZTCW.

6. Sizov V.A. Development of models of an analytical data processing system for monitoring the information security of an informatization object using cloud infrastructure / V.A. Sizov, A.D. Kirov // Russian Technological Journal. – 2021. – pp. 16-25.
7. How MITRE ATT and SK technicians introduce positive technologies. – URL: https://mitre.ptsecurity.com/ru-RU/techniques?utm_source=seclab&utm_medium=news (accessed: 1.03.2024)
8. Onyango, Oscar. Artificial intelligence and its application for information security management / Onyango, Oscar. 10.13140/RG.2.2.12066.09921.
9. Sidorova, D. N. Algorithms and methods of data clustering in the analysis of information security event logs / D. N. Sidorova, E. N. Pivkin // Security of digital technologies. – 2022. – № 1(104). – Pp. 41-60. – DOI 10.17212/2782-2230-2022-1-41-60. – REGISTRATION NUMBER RMDHEC.
10. PT Expert Security Center. – URL: https://www.ptsecurity.com/ru-ru/services/esc / (accessed: 1.03.2024)
11. Yosang A. Subjective logic. A formalism for reasoning under conditions of uncertainty. – Springer International Publishing House, Switzerland, 2016. – 337 p. ISBN 978-3-319-42335-7(1). DOI 10.1007/ 978-3319-42337-1.
12. Park Yu. On the optimality of the analysis of trust networks using subjective logic. Achievements in the field of electrical and computer engineering, 14(3):49-54, 2014.
13. MITRE ATT&CK. – URL: https://attack.mitre.org / (accessed: 1.03.2024)



**Для цитирования:** Киров, А.Д., ПРИМЕНЕНИЕ МОДЕЛИ ОЦЕНКИ ДОВЕРИЯ НА ОСНОВЕ СУБЪЕКТИВНОЙ ЛОГИКИ К СОБЫТИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КИБЕРИГРАХ// Научный сетевой журнал «Столыпинский вестник» №5/2024.