Научная статья
Original article
УДК 332.3
doi: 10.55186/2413046X_2024_9_5_255

К ВОПРОСУ СНИЖЕНИЯ КОЛИЧЕСТВА ЧС НА ТЕХНОЛОГИЧЕСКИХ СИСТЕМАХ АГРОПРОМЫШЛЕННЫХ КОМПЛЕКСОВ

ON THE ISSUE OF REDUCING THE NUMBER OF EMERGENCIES IN THE TECHNOLOGICAL SYSTEMS OF AGRO-INDUSTRIAL COMPLEXES

Чибинёв Николай Николаевич, доцент, Южно-Российский государственный политехнический университет (НПИ) им. М.И. Платова, Новочеркасск, Российская Федерация, e-mail: fire.expert.ug@gmail.com

Яковенко Елена Александровна, доцент, Южно-Российский государственный политехнический университет (НПИ) им. М.И. Платова, Новочеркасск, Российская Федерация, e-mail: yakovlena80@yandex.ru

Федоров Виктор Матвеевич, профессор, Новочеркасский инженерно-мелиоративный институт им. А.К. Кортунова - филиал Донского государственного аграрного университета, Новочеркасск, Российская Федерация

Chibinev Nikolay Nikolaevich, Associate Professor, South Russian State Polytechnic University (NPI) named after. M.I. Platova, Novocherkassk, Russian Federation, e-mail: fire.expert.ug@gmail.com

Yakovenko Elena Aleksandrovna, Associate Professor, South Russian State Polytechnic University (NPI) named after. M.I. Platova, Novocherkassk, Russian Federation, e-mail: yakovlena80@yandex.ru

Fedorov Viktor Matveyevich, Professor of the A. K. Kortunov Novocherkassk Engineering and Reclamation Institute-branch of the Don State Agrarian University, Novocherkassk, Russian Federation, e-mail: viktor-fedorov1955@yandex.ru

Аннотация. Актуальность. Развитое сельское хозяйство России — это залог продовольственной безопасности страны в целом и каждого её региона в отдельности. При этом АПК являются стратегически значимыми отраслями в государстве, так как крупные агрохолдинги в настоящее время являются основными поставщиками продовольствия населению в нашей стране. Особенно опасны кибератаки на объекты фермерских хозяйств так как вмешательство и взлом высокотехнологичного оборудования и программного обеспечения непосредственно приводит к сбоям в работе АПК и сельских хозяйств. **Объект.** Объектом исследований являются технологические системы агропромышленного комплекса. **Материалы и методы.** Входе исследования проведен анализ последствий кибератак, выявлены уязвимости и "взломанные" защитные меры на объектах сельского хозяйства в нашей стране. Использовались методы обобщения, обработки и анализа статистических данных о чрезвычайных ситуациях, причинами которых стали кибератаки. Научные методы исследования концентрировались на сравнительном анализе, с помощью которого выявлены актуальность и проблематика современных угроз киберпреступности в агропромышленном комплексе (АПК) и систематизацию, позволившую сформулировать выводы и предложения по предупреждению кибератак на сельскохозяйственные объекты экономики с учётом современных тенденций развития IT-технологий. **Результаты и выводы.** Исследованиями установлены типичные уязвимости компьютерных сетей, такие как использование устаревших систем, недостаточная сетевая сегментация и слабые аутентификационные меры при обеспечении безопасности технологий и охраны труда в механизированном

агропромышленном производстве. Проанализированы причины успешных хакерских "взломов", к которым относятся недостаточное осознание рисков, отсутствие системы мониторинга и своевременного реагирования. Результаты исследования обуславливают необходимость постоянного развития методов и стратегий обеспечения информационной безопасности на объектах сельскохозяйственного производства.

Abstract. Relevance. The developed agriculture of Russia is the key to the food security of the country as a whole and of each of its regions individually. At the same time, agro-industrial complex are strategically important industries in the state, since large agricultural holdings are currently the main suppliers of food to the population in our country. Cyber attacks on farm facilities are especially dangerous, as interference and hacking of high-tech equipment and software directly leads to disruptions in the work of agriculture and agriculture. An object. The object of research is the technological systems of the agro-industrial complex. Materials and methods. The results of the study analyzed the consequences of cyber attacks, identified vulnerabilities and "hacked" protective measures at agricultural facilities in our country. The methods of generalization, processing and analysis of statistical data on emergency situations, the causes of which were cyber attacks, were used. Scientific research methods focused on comparative analysis, which revealed the relevance and problems of modern cybercrime threats in the agro-industrial complex (AIC) and systematization, which allowed to formulate conclusions and proposals for the prevention of cyber attacks on agricultural facilities of the economy, taking into account current trends in the development of IT technologies. Results and conclusions. Studies have established typical vulnerabilities of computer networks, such as the use of outdated systems, insufficient network segmentation and weak authentication measures to ensure the safety of technologies and occupational safety in mechanized agro-industrial production. The reasons for successful hacker "hacks" are analyzed, which include insufficient awareness of risks, lack of a monitoring system and timely response.

The results of the study necessitate the constant development of methods and strategies for ensuring information security at agricultural production facilities.
Ключевые слова: сельское хозяйство, агропромышленный комплекс, чрезвычайная ситуация, уязвимость, стратегии безопасности, технологические системы, мониторинг безопасности

Keywords: agriculture, agro-industrial complex, emergency, vulnerability, security strategies, technological systems, security monitoring

Введение. В настоящее время в России наблюдается всплеск кибератак, направленных в основном на подрыв безопасности информационных систем государственных учреждений, телекома и сельского хозяйства [1,2]. Катастрофически опасны кибератаки на информационные системы государственных учреждений, телекома и объектов сельского хозяйства по причине возникновения различных видов чрезвычайных ситуаций.

Особенно опасны кибератаки на объекты агропромышленного комплекса и фермерских хозяйств нашей страны так как постороннее вмешательство и взлом высокотехнологичного оборудования и программного обеспечения в сельскохозяйственном производстве непосредственно приводит к сбоям в работе АПК и фермерских хозяйств, использующих искусственный интеллект. Кибератака представляет собой искажение набора программных данных или полного отключения различного сельскохозяйственного оборудования, автономных дронов и роботизированных комбайнов [4], что ведет [5]:

- к порче сельскохозяйственной продукции и финансовым потерям;
- к остановкам в работе производств и ошибкам в логистике при доставке продуктов питания;
- к возникновению товарного дефицита и провокации роста цен на сельхозпродукты;

- к уменьшению или полной потере имиджа сельхозпроизводства и конкретного сельхозпроизводителя;
- к подрыву доверия потребителей и социальным волнениям в стране.

Характерными резонансными кибератаками на сельхозпроизводителей России в 2022-2023 годах были:

В феврале 2022 года хакеры-злоумышленники совершили несанкционированный доступ к ключевым системам в агрохолдинге «Селятино» и попытались испортить 40 тонн продукции, изменив температуру хранения замороженной продукции на плюсовую [6].

В марте 2022 года агрохолдинг «Мираторг» подвергся кибератаке, в следствии чего 18 предприятий агрохолдинга не могли оформлять производственные и транспортные ветеринарные документы на продукцию [7].

В марте этого года из-за кибератаки на серверы, рабочие станции и информационные системы предприятия была временно остановлена работа колбасного завода «Тавр» в Ростовской области [8].

Более 20 раз с апреля 2023 года подвергался кибератакам сервис «АгроСигнал» российской компании «ИнфоБис», которая занимается разработкой и внедрением информсистем в сельском хозяйстве для повышения качественных характеристик продукции растениеводства [10].

Вице-премьер РФ Чернышенко Д.Н. 3 марта 2023 году в Уфе на встрече с молодыми учеными, изобретателями и технологическими предпринимателями Евразийского НОЦ мирового уровня сообщил, что в 2022 году было отражено около 50 000 хакерских атак на российские интернет-ресурсы и число кибератак в 2023 году на российские системы выросло на 65% [11]. Более 170 кибератак на Россию каждый день регистрирует ИБ-центр ФСБ, после начала специальной военной операции на Украине [12].

Основной особенностью кибератак, создавших киберЧС, является их скорость распространения, которая может быть как внезапная, так и по происшествии некоторого времени. Это значит, что разрушающее программное средство может существовать в компьютерной системе, не проявляя себя, до наступления определённого события, даты или свершения запрограммированного действия, а может причинять вред сразу с момента проникновения в систему. До того, как разрушающее программное средство себя проявит, логику его действий предсказать весьма трудно.

Это подчеркивает безотлагательную необходимость использовать современные IT- решения для борьбы с киберпреступленностью в сельскохозяйственном производстве.

Материалы и методы. Целью данного исследования является анализ технологических аспектов обеспечения информационной безопасности на объектах АПК и фермерских хозяйствах с акцентом на шифрование данных и коммуникаций, аутентификацию и авторизацию, мониторинг и анализ безопасности, а также защиту от вредоносных программ. Данная проблема рассматривалась с точки зрения защищенности информации и безопасности сельскохозяйственных технологических процессов и производств. Для решения поставленной задачи научные методы исследования концентрировались на сравнительном анализе современных угроз киберпреступности в АПК и систематизацию, позволившую сформулировать выводы и предложения по предупреждению киберчрезвычайных ситуаций на объектах АПК и фермерских хозяйствах с учётом современных тенденций развития IT-технологий. В процессе отбора статистических данных использовались методы как сплошного, так и выборочного исследования.

Результаты и обсуждение. В ходе исследования нами был проведен анализ последствий кибератак, нацеленных на технологические системы АПК и фермерские хозяйства, который выявил следующие типичные уязвимости и уровни защиты, которые были нарушены:

1. Слабые аутентификационные меры - отсутствие двукратной аутентификации или использование слабых паролей упрощает задачу хакерам.

2. Недостаточная сетевая сегментация - в некоторых случаях, производственные сети были недостаточно разделены от корпоративных сетей, что позволило злоумышленникам распространить свой доступ.

3. Устаревшие системы и ПО - применение устаревших операционных систем и программного обеспечения с неустранимыми уязвимостями облегчает их взлом.

4. Необновляемые устройства - продолжительное использование устройств с истекшими сроками обновления без патчей делает системы уязвимыми.

По результатам исследования установлен ряд коренных причин, по которым «реализованные» кибератаки на технологические системы сельскохозяйственных объектов становились возможными:

1. Недостаточное осознание рисков – во многих отраслях сельского хозяйства недооценивают угрозы кибербезопасности и не принимают соответствующих мер предосторожности.

2. Отсутствие системы мониторинга и реагирования - большинство объектов АПК и особенно фермерских хозяйств не имели эффективных систем мониторинга и быстрого реагирования на киберугрозы.

3. Недостаточное внимание к персоналу - социальная инженерия и фишинг-атаки оказались реализованными из-за недостаточной обученности IT – персонала в области кибербезопасности сельскохозяйственных объектов.

4. Скрытие совершённых кибератак – из-за боязни потерять имидж сельхозпроизводителя и рынка сбыта продукции.

5. Неактуальные политики безопасности - отсутствие актуальных и строгих политик в области кибербезопасности в отраслях сельского хозяйства позволило злоумышленникам действовать не замеченными.

На государственном уровне в России в настоящее время общепринятого понимания «киберчрезвычайной ситуации» не существует, что не позволяет эффективно проводить организационные и аварийно-спасательные работы на объектах АПК и фермерских хозяйствах.

Данный анализ позволил сделать следующие выводы и определить уязвимости компьютерных систем, которые были использованы злоумышленниками на объектах сельского хозяйства России.

Заключение

1. Неукоснительно исполнять Указ Президента Российской Федерации № 166 от 30.03.2022 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» с 1 января 2025 года не допускать использование иностранного программного обеспечения на объектах критической инфраструктуры, принадлежащей госорганам [13, 14].

2. Установлено, что основными методами обеспечения информационной безопасности в настоящее время являются: криптография [15], идентификация и аутентификация [16], брандмауэры и системы обнаружения вторжений [17], которые учтены в современной системе защиты в модели Zero Trust [18], а технологическими решениями для управления информационной безопасностью являются: системы управления доступом [19], средства мониторинга и аудита [20] и облачные технологии для информационной безопасности .

3. Для эффективного обеспечения безопасности компьютерных систем АПК и фермерских хозяйств необходимо сформировать модель угроз технологической безопасности для их программного обеспечения. Моделью будет являться официально принятый корпоративный нормативно-технический документ, которым обязаны руководствоваться как сами заказчики, так и разработчики программных комплексов для отраслей сельского хозяйства.

4. Так как методы обеспечения и управления информационной безопасности являются только одним из элементов в общей стратегии обеспечения безопасности сельскохозяйственных объектов, то следует уделять постоянное внимание обучению IT- сотрудников данных объектов.

5. Из-за отсутствия международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, назрела острая необходимость принятия специального отраслевого законодательного документа, определяющего правовые и организационные основы борьбы с чрезвычайными ситуациями от кибератак в отраслях сельского хозяйства России.

Список источников

1. ГК «Солар» рассказала о топ-10 атакуемых отраслей в 2023 году [электронный ресурс] https://habr.com/ru/news/773892/ГК

2. Никульченкова Е. В. Трансформация киберпреступности: современные угрозы и их предупреждение // Вестник Омского университета. Серия «Право». 2023. Т. 20, № 3. С. 96-105. DOI: 10.24147/1990-5173.2023.20(3).96-105.

3. Федеральный закон от 29.12.2006 N 264-ФЗ (ред. от 04.08.2023) "О развитии сельского хозяйства".

4. Указ Президента Российской Федерации от 10 октября 2019 г. № 490 "О развитии искусственного интеллекта в Российской Федерации".

5. Сельское хозяйство и кибератаки [электронный ресурс] https://www.tt9.by/articles/selskoe-hozyaystvo-i-kiberataki

6. Anonymous пытались испортить 40 тысяч тонн продукции в агрохолдинге Селятино [электронный ресурс] https://www.securitylab.ru/news/530388.php

7. Агрохолдинг "Мираторг" подвергся атаке шифровальщика [электронный ресурс] https://www.itsec.ru/news/agroholding-miratorg-podvergsia-atake-shifrovalshika

8. Крупнейший на юге производитель мясных продуктов «Тавр» подвергся хакерской атаке [электронный ресурс] https://www.expertsouth.ru/news/krupneyshiy-na-yuge-proizvoditel-myasnykh-produktov-tavr-podvergsya-khakerskoy-atake

9. Хакеры приступили к сбору урожая Хакеры приступили к сбору урожая https://www.kommersant.ru/doc/6095159

10. Город Окленд в США объявил режим ЧС после кибератаки Хакеры приступили к сбору урожая https://www.securitylab.ru/news/536498.php

11. Центр по компьютерным инцидентам фиксирует более 170 кибератак на РФ ежедневно Хакеры приступили к сбору урожая https://www.interfax.ru/digital/903202

12. Указ Президента Российской Федерации № 166 от 30.03.2022 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»

13. Указ Президента Российской Федерации от 1 мая 2022 г. № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации"

14. Мировые тенденции криптографической защиты данных 2012. Исследование Thales e-Security Хакеры приступили к сбору урожая https://pr.adcontext.net/13/05/29/144761

15. исследование 2021 State of Password and Authentication Security Behaviors Report от компании LastPass

16. Отчет "2021 SonicWall Cyber Threat Report

17. Zero Trust: новый подход к информационной безопасности Хакеры приступили к сбору урожая https://in4security.com/news/tpost/hbtpa5up11-zero-trust-novii-podhod-k-informatsionno

18. Исследование 2021 Identity and Access Management Report

19. Отчет 2021 SANS Cyber Threat Intelligence Survey

20. Отчет 2021 Cloud Security Report от компании Cybersecurity Insiders

References

1. Solar Group told about the top 10 attacked industries in 2023 [electronic resource] https://habr.com/ru/news/773892/ГК

2. Nikulchenkova E. V. Transformation of cybercrime: modern threats and their prevention // Bulletin of Omsk University. The series "Law". 2023. Vol. 20, No. 3. pp. 96-105. DOI: 10.24147/1990-5173.2023.20(3) .96-105.

3. Federal Law No. 264-FZ of 12/29/2006 (as amended on 08/04/2023) "On the development of agriculture".

4. Decree of the President of the Russian Federation No. 490 dated October 10, 2019 "On the development of artificial intelligence in the Russian Federation".

5. Agriculture and cyber attacks [electronic resource] https://www.tt9.by/articles/selskoe-hozyaystvo-i-kiberataki

6. Anonymous tried to spoil 40 thousand tons of products in Selyatino agricultural holding [electronic resource] https://www.securitylab.ru/news/530388.php

7. Miratorg agroholding was attacked by a cryptographer [electronic resource] https://www.itsec.ru/news/agroholding-miratorg-podvergsia-atake-shifrovalshika

8. The largest producer of meat products in the south, Tavr, was subjected to a hacker attack [electronic resource] https://www.expertsouth.ru/news/krupneyshiy-na-yuge-proizvoditel-myasnykh-produktov-tavr-podvergsya-khakerskoy-atake

9. Hackers have started harvesting Hackers have started harvesting https://www.kommersant.ru/doc/6095159

10. The city of Oakland in the USA declared an emergency mode after a cyber attack, Hackers began harvesting https://www.securitylab.ru/news/536498.php

11. The Center for Computer Incidents records more than 170 cyber attacks on the Russian Federation every day, Hackers have begun harvesting https://www.interfax.ru/digital/903202

12. Decree of the President of the Russian Federation No. 166 dated 30.03.2022 "On measures to ensure the technological independence and security of the critical information infrastructure of the Russian Federation"

13. Decree of the President of the Russian Federation No. 250 dated May 1, 2022 "On additional measures to ensure information security of the Russian Federation"
14. Global trends in cryptographic data protection 2012. Thales e-Security Research Hackers have started harvesting https://pr.adcontext.net/13/05/29/144761
15. The 2021 State of Password and Authentication Security Behaviors Report from LastPass
16. Report "2021 SonicWall Cyber Threat Report
17. Zero Trust: a new approach to information security Hackers have started harvesting https://in4security.com/news/tpost/hbtpa5up11-zero-trust-novii-podhod-k-informatsionno
18. The 2021 Identity and Access Management Report
19. Report 2021 SANS Cyber Threat Intelligence Survey
20. The 2021 Cloud Security Report from Cybersecurity Insiders
© Чибинёв Н.Н., Яковенко Е.А., Федоров В.М., 2024. Московский экономический журнал, 2024, № 5.