2021
Итоги

CYBER SECURITY UZ

Обеспечение кибербезопасности в Республике Узбекистан

info@csec.uz
(55) 502-10-10
www.csec.uz

Содержание

Введение

Число пользователей киберпространства в мире растет изо дня в день, это обусловлено высоким темпом роста и спроса на информационно-коммуникационные услуги.

Узбекистан не стал исключением, только в 2021 году выполнены многочисленные проекты по широкому внедрению информационно-коммуникационных технологий в сферы деятельности органов государственного и хозяйственного управления, государственной власти на местах и иными организациями.

Все используемые в Узбекистане и мире информационно-коммуникационные технологии и оборудование в совокупности является киберпространством. Такое развитие имеет и оборотную сторону – киберпреступность, дающая злоумышленникам новые и изощренные способы вымогательства денежных средств, использования киберпространства в злонамеренных целях.

Стоит отметить, что уровень киберпреступности увеличивается в результате отсутствия примитивных мер защиты информационных систем и ресурсов, а также низкого уровня обеспечения кибербезопасности.

Угрозы

В Узбекистане по состоянию на 2021 год зарегистрировано 100 015 доменов национального сегмента сети Интернет «.uz», из которых порядка 38 000 являются активными. Из 38 000 активных доменов всего 14 014 являются защищенными, т.е. имеют SSL-сертификат безопасности. В остальных случаях, либо сертификат является просроченным – 613 случаев, либо отсутствует (Рис. 1).

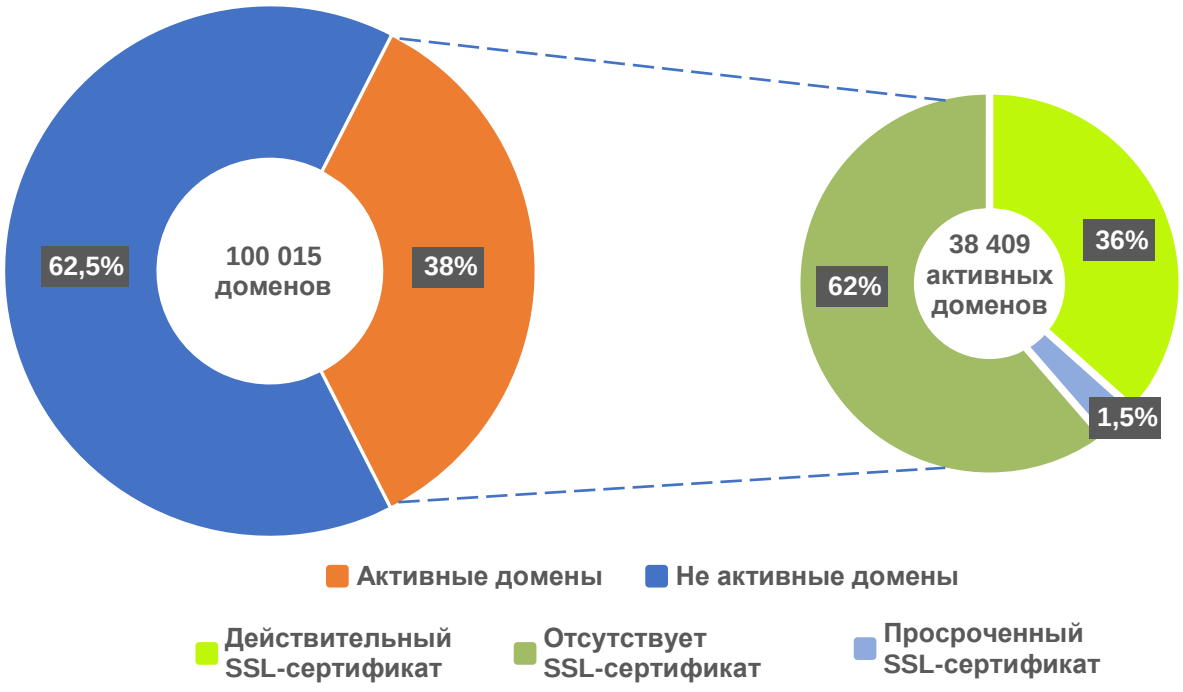

Рис. 1. Информация о доменах и наличии сертификата безопасности.

В 2021 году Центром выявлено 17 097 478 случаев вредоносной и подозрительной сетевой активности, исходящей из адресного пространства национального сегмента сети Интернет (Рис. 2).

Большая часть данной активности, а именно 76% составляют участники бот-сетей.

Рис. 2. Основные виды выявленных угроз.

Основное количество вредоносной и подозрительной сетевой активности исходило от пользователей Национальных операторов и провайдеров (Рис. 3).

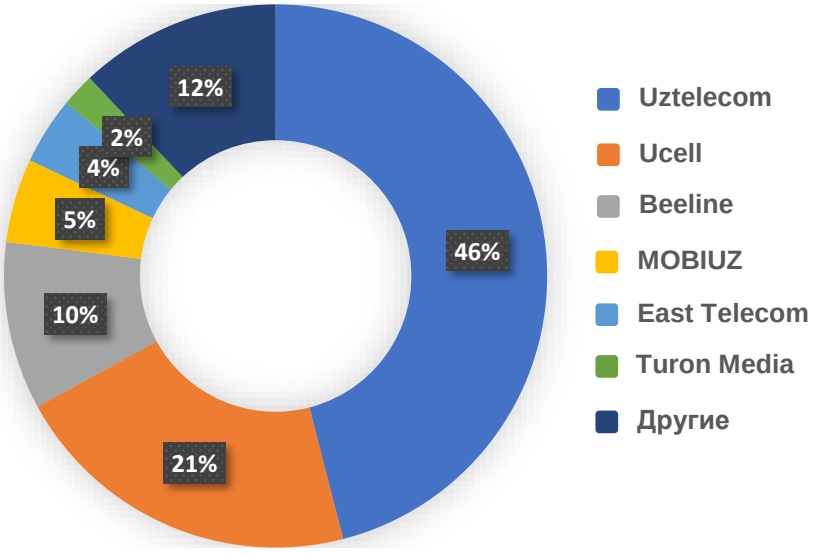

Рис. 3. Выявленные случаи вредоносной сетевой активности, в разрезе операторов и провайдеров.

В частности, при сравнении с аналогичным периодом 2020 года (более 20 млн. киберугроз) количество киберугроз кибербезопасности уменьшилось **на 20 %**, за счёт скоординированных мер по реагированию на выявленные уязвимости кибербезопасности и сетевые аномалии.

Кроме этого, при помощи системы защиты веб-приложений Центра выявлено и отражено 1 354 106 кибератак (Рис. 4) совершенных в отношении веб-сайтов национального сегмента сети Интернет.

Рис. 4. Выявленные и отраженные кибератаки.

Наибольшее количество кибератак было совершено с территории Узбекистана, Российской Федерации, Германии и т.д. (Рис. 5).

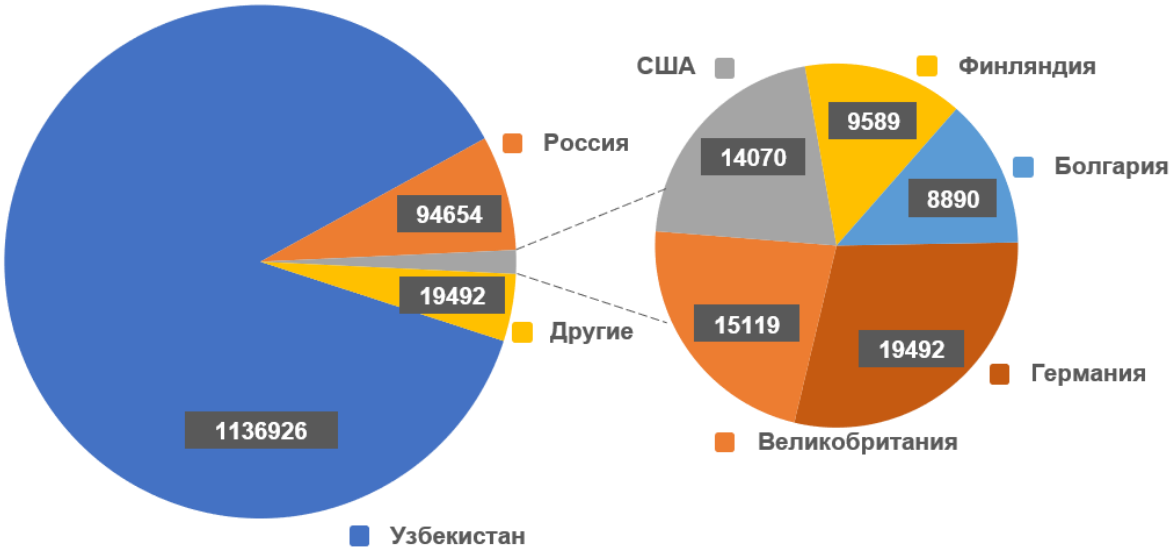

Рис. 5. Страны с адресного пространства которых осуществлялись кибератаки.

Инциденты и события

В рамках безопасного функционирования веб-сайтов государственных органов (круглосуточный мониторинг событий

и инцидентов безопасности), за 2021 год выявлено 636 событий безопасности (Рис. 6), что составляет порядка 1 048 216 минут недоступности (простоя) веб-сайтов органов государственного и хозяйственного управления, государственной власти на местах и иных организаций.

Рис. 6. Основные виды выявленных событий.

В ходе мониторинга информационных систем государственных органов, подключенных к межведомственной сети передачи данных (МСПД), зафиксировано 33 317 648 событий безопасности, из которых 347 742 событий могли привести к несанкционированному получению доступа и утечке конфиденциальной информации (Рис. 7).

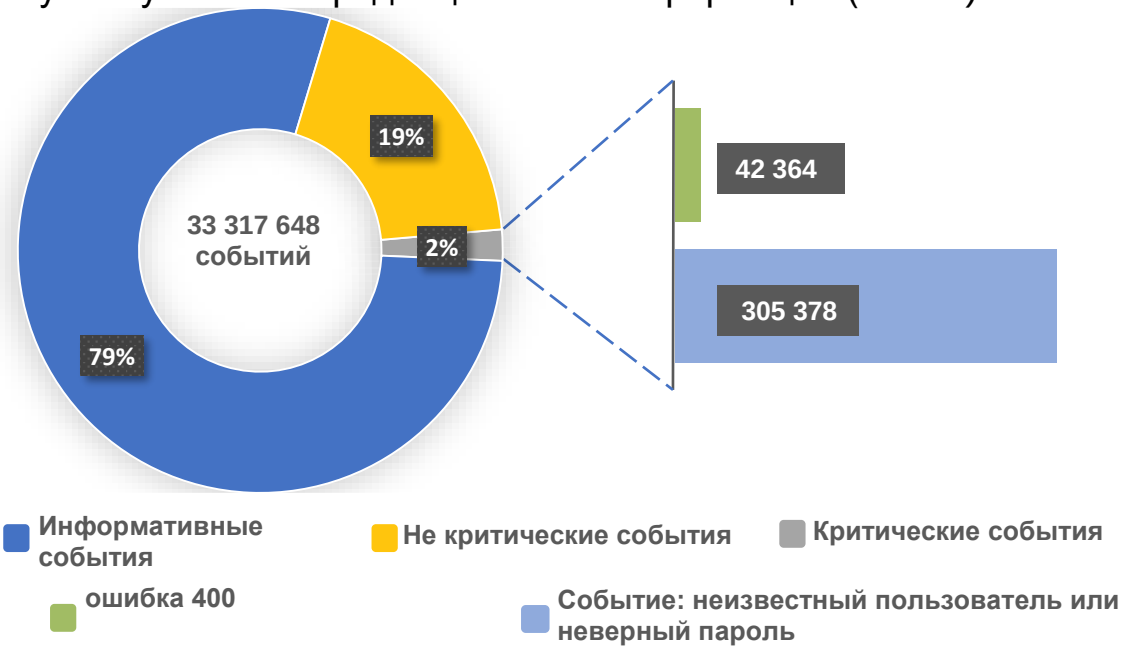

Рис. 7. Выявленные события в информационных системах.

По итогам мониторинга инцидентов кибербезопасности, совершенных в отношении веб-сайтов доменной зоны «UZ», зафиксировано 444 инцидента, из которых наибольшее количество приходится на несанкционированную загрузку контента (НЗК) – 341 и несанкционированное изменение главной страницы (Deface) – 89 (Рис. 8).

Анализ инцидентов показал, что веб-сайты государственного сектора (134 инцидент) подвержены атакам в 3 раза реже, по сравнению с частным сектором (310 инцидент).

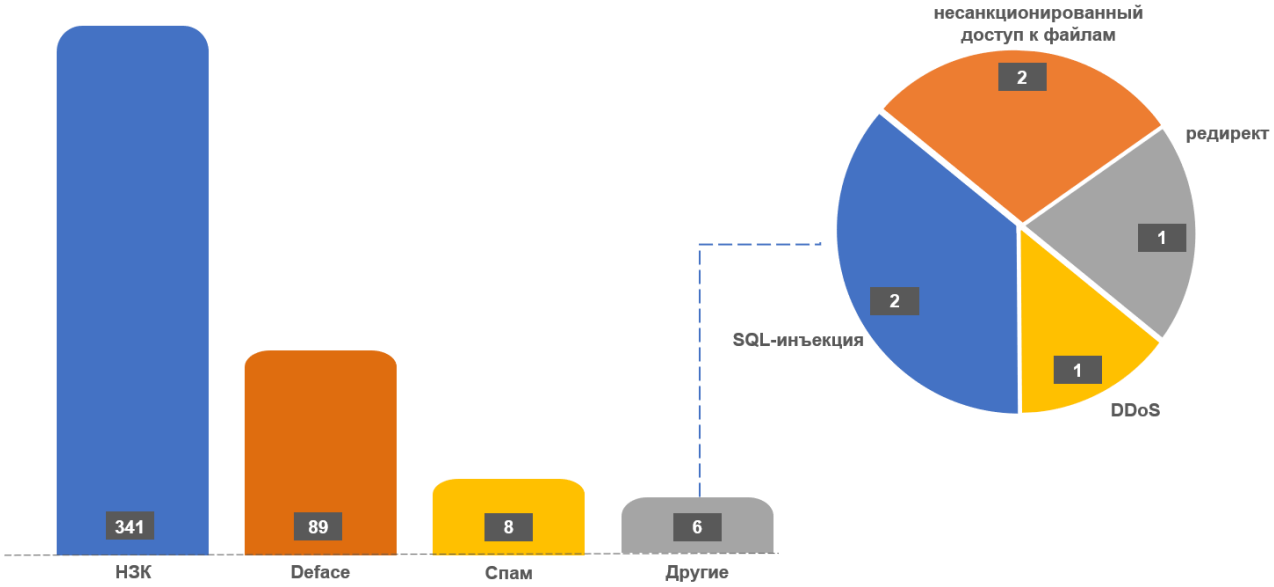

Рис. 8. Инциденты кибербезопасности веб-сайтов.

Детальный анализ инцидентов показал, что наиболее уязвимыми (часто атакуемые) являются веб-сайты разработанные на системах управления контентом «Wordpress», «Joomla», «Open Journal Systems» и «Drupal» (Рис. 9).

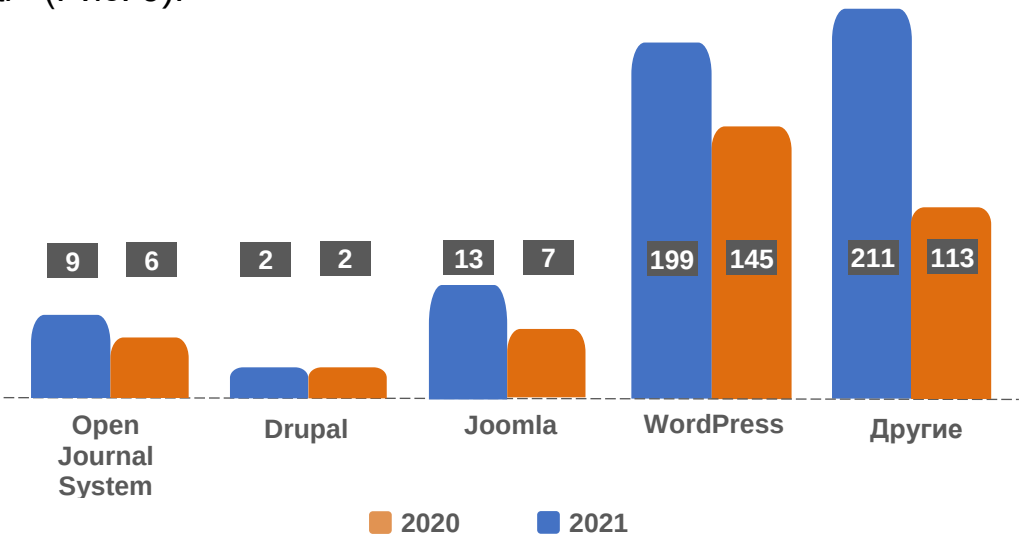

Рис. 9. Сравнение инцидентов 2021 и 2020 годов.

Расследование инцидентов кибербезопасности

В рамках выявления вредоносного контента и анализа его причастности к правонарушениям в информационном пространстве

проведены расследования инцидентов кибербезопасности, в ходе которых установлены причины и способы их осуществления.

Основными причинами и способами успешной реализации хакерских атак являются: наличие уязвимостей в веб-приложениях, в частности из-за несвоевременного их обновления (72%), использование слабых паролей (25%) и другие.

В частности, по итогам расследований выявлено 6 635 вредоносных файлов и скриптов, представляющих угрозы кибербезопасности для информационных систем и ресурсов, а также их пользователей (Рис. 10).

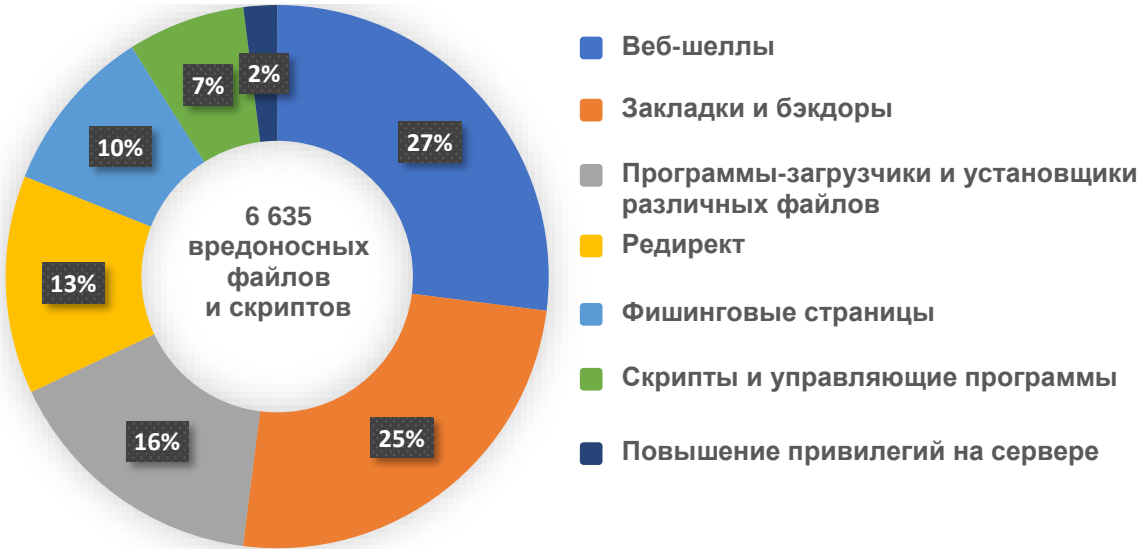

Рис. 10. Основные группы выявленных вредоносных файлов и скриптов.

Наряду с этим определено, что в 97% случаев источниками неправомерной активности являются адресные пространства зарубежных стран. В частности, наибольшее количество случаев неправомерной активности связано со следующими странами: США, Индонезия, Нидерланды, Румыния, Алжир и Тунис. При этом, необходимо помнить, что злоумышленники пользуются прокси-сервисами для скрытия своего истинного местонахождения и используют цепочки прокси-серверов для усложнения их поиска.

Такое большое количество неправомерной активности в адресном пространстве Республики обусловлено пренебрежением большинства собственников и администраторов национальных информационных систем и ресурсов требованиями информационной и кибербезопасности, что существенно повышает риск несанкционированного вмешательства в их работу.

Уязвимости

В ходе выполнения мероприятий по повышению уровня защищенности национальных информационных систем и ресурсов за 2021 год проведено 256 изучений и экспертиз.

По итогам проведенных работ выявлено 989 уязвимостей кибербезопасности (Рис. 11), о наличии которых своевременно были оповещены владельцы информационных систем и ресурсов:

– высокого уровня критичности – 683;
– среднего уровня критичности – 271;
– низкого уровня критичности – 35.

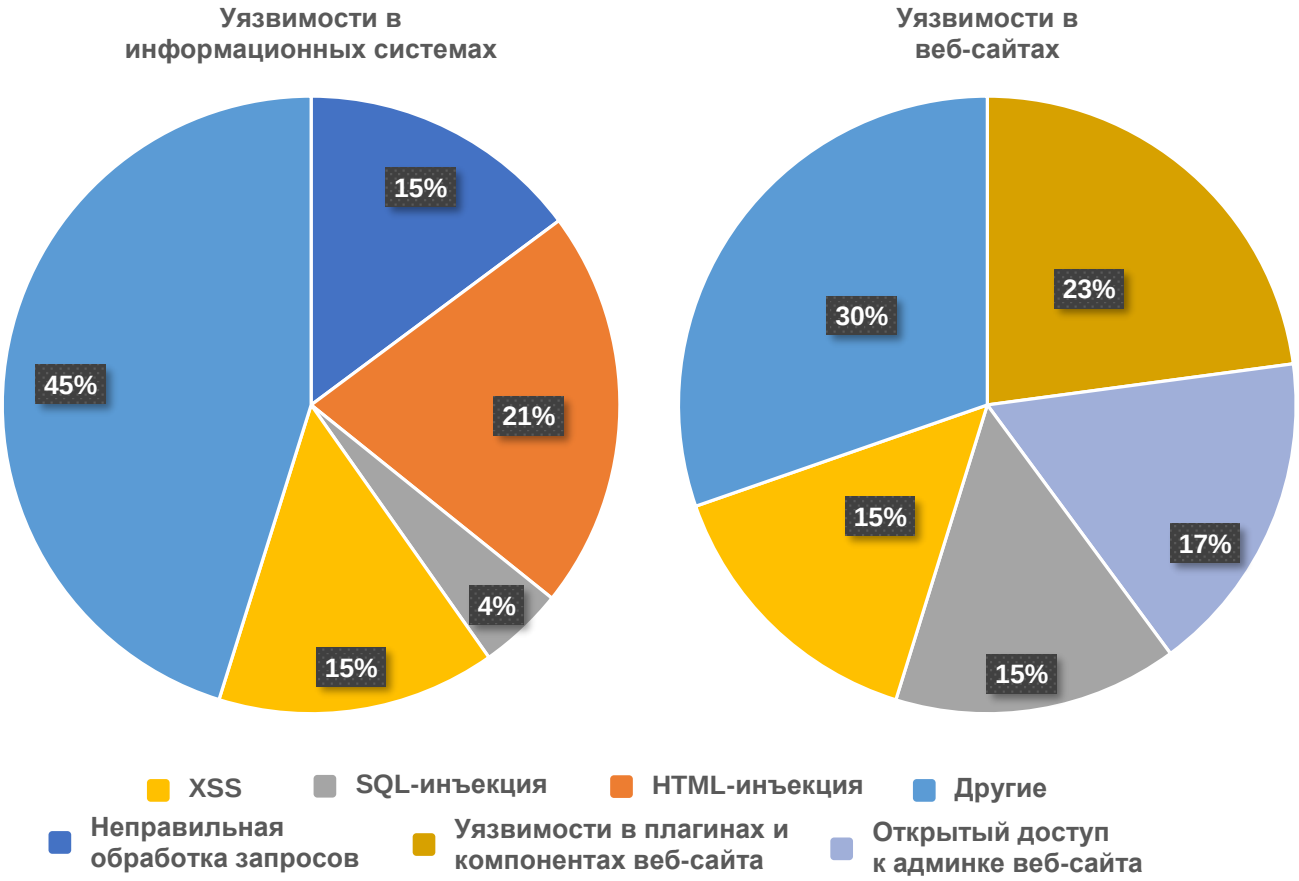

Рис. 11. Основные виды выявленных уязвимостей.

Эксплуатация злоумышленниками вышеописанных уязвимостей могла привести к нарушению целостности и доступности информационных ресурсов, в том числе к утечке персональных данных граждан Республики Узбекистан.

Сертификация

В целях подтверждения качества систем управления информационной безопасности, аппаратных средств, программных продуктов, информационно-коммуникационных технологий, телекоммуникационного оборудования и иных технических средств, в том числе средств защиты информации, проведена сертификация 21 программного продукта, а также 3 аппаратно-программных средств иностранного и отечественного происхождения на соответствие требованиям нормативных документов по информационной и кибербезопасности (Рис. 12).

Рис. 12. Сертифицированное программное обеспечение.

Заключение

Все вышесказанное свидетельствует об обострении киберугроз в Узбекистане. И не трудно сделать выводы, что на сегодняшний день стоит уделять особое внимание безопасности в киберпространстве, в частности повышение уровня защищенности и обеспечения кибербезопасности информационных систем и веб-сайтов, а также регулярно повышать уровень знаний пользователей в сфере информационно-коммуникационных технологий и информационной безопасности.

Наряду с этим, рекомендуется:

1. Использовать лицензионные и сертифицированные операционные системы, и программное обеспечение.
2. Регулярно обновлять и следить за актуальностью версий используемых операционных систем, программного обеспечения и компонентов безопасности. Обновление производить из официальных источников.
3. Использовать плагины безопасности с функциями поиска, удаления и защиты в дальнейшем от вредоносных программ.
4. Регулярно проводить работы по резервному копированию баз данных, файлов, почты и прочее.
5. Удаление неиспользуемых плагинов – любой новый плагин или расширение увеличивает вероятность риска атаки со стороны злоумышленников. В этой связи, рекомендуется отключить и удалить неиспользуемые плагины и по возможности использовать встроенные механизмы вместо установки плагина на каждый частный случай.
6. Усилить парольную аутентификацию – для административного аккаунта, личного кабинета на сайте сервис-провайдера и учётной записи на сервере (например, для выделенного или «co-location» хостинга)

настоятельно рекомендуется использовать сложный и неповторяющийся пароль. При изменении пароля рекомендуется использовать правила формирования паролей для учетных записей, предусматривающую генерацию паролей с использованием цифр, специальных символов, букв верхнего и нижнего регистра с минимальной длинной в 8 символов. Рекомендуется настроить двухфакторную аутентификацию (при наличии такой возможности). Также рекомендуется установить ограничение количества попыток входа (защита от атак методом перебора паролей, «bruteforce»).

7. Осуществлять доступ к информационной системе или веб-сайту осуществлять с устройств (компьютеры, планшеты), на которых установлены антивирусные программные средства с актуальными базами вирусных сигнатур.

8. Периодически проводить экспертизы на соответствие требованиям обеспечения кибербезопасности информационных систем и ресурсов. Своевременное устранять выявленные уязвимости на основании рекомендаций, направленных по итогам проведенных экспертиз.

9. Регулярно повышать квалификацию и уровень знаний в сфере информационно-коммуникационных технологий и информационной безопасности пользователей (сотрудников).

10. Оперативно реагировать и принимать соответствующие меры по устранению угроз и ликвидации последствий на инциденты кибербезопасности.

Принятие вышеуказанных и других дополнительных мер защиты позволит существенно снизить риски возникновения угроз кибербезопасности, что в свою очередь даст возможность оградить себя от вероятных атак и последующей необходимости устранять причины и последствия инцидентов информационной безопасности.